AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 115–475

# MITIGATING AMERICA'S CYBERSECURITY RISK

## HEARING

BEFORE THE

## COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

APRIL 24, 2018

Available via the World Wide Web: http://www.govinfo.gov

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
32–454 PDF WASHINGTON : 2019

## COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

JOHN McCAIN, Arizona<br>
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
JOHN HOEVEN, North Dakota
STEVE DAINES, Montana

CLAIRE McCASKILL, Missouri
THOMAS R. CARPER, Delaware
HEIDI HEITKAMP, North Dakota
GARY C. PETERS, Michigan
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
DOUG JONES, Alabama

Christopher R. Hixon, *Staff Director*
Gabrielle D'Adamo Singer, *Chief Counsel*
Colleen E. Berny, *Research Assistant*
Margaret E. Daum, *Minority Staff Director*
Julie G. Klein, *Minority Professional Staff Member*
Laura W. Kilbride, *Chief Clerk*
Bonni E. Dinerstein, *Hearing Clerk*

# CONTENTS

## WITNESSES

### Tuesday, April 24, 2018

### Alphabetical List of Witnesses

## APPENDIX

# MITIGATING AMERICA'S CYBERSECURITY RISK

## TUESDAY, APRIL 24, 2018

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
*Washington, DC.*

The Committee met, pursuant to notice, at 10 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Lankford, Hoeven, Daines, McCaskill, Carper, Heitkamp, Peters, Hassan, Harris, and Jones.

## OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. Good morning. This hearing will come to order.

I want to welcome our witnesses. Thank you for your time, your thoughtful written testimony, and looking forward to you answering our questions.

The hearing is called "Mitigating America's Cybersecurity Risk." I will first ask that my written opening statement be entered into the record.[1]

I think the word "mitigating" is a good one. We are not going to solve this problem. The people on offense are continuing to increase their capabilities. I remember being briefed a couple of years ago about North Korea's capability. The consensus was they are far behind, for example, Russia and China. Now it sounds like they have really upped their game. They are always on the offense, they are always developing new tools, and we are playing defense and we are behind. I think we have to look at mitigating.

I am mindful of the fact that the Department of Homeland Security (DHS) is very disappointed that we were not able to include in the omnibus the renaming of the National Protection and Programs Directorate (NPPD). I do not know who ever came up with that name. But, obviously, Cybersecurity and Infrastructure Security Agency (CISA) would be a better name for it.

From my standpoint, it is bizarre, it is ridiculous that it requires an act of Congress for the Department of Homeland Security to rename an agency and restructure it so it actually does a better job. I do not get that, but that is the way it is. I do not know what the objection was. I think that might indicate further future problems in terms of lack of cooperation and coordination within the agen-

[1] The prepared statement of Senator Johnson appears in the Appendix on page 51.

cies, within committees, within Congress. But it is just unfortunate. We are going to do everything we can. Maybe a really good solution would be to pass the DHS authorization bill through the Senate that we passed through our Committee that includes that as well. But if that does not work, we will try and figure something out.

We have passed a number of laws. I got here in 2011, and from day one everybody recognized cybersecurity is an issue, and it always kind of scares me when I hear this: "We have to do something about it." Well, we have been doing things about it. We have been passing laws. I think we have plenty of laws on the books. I really do. The question is: Are we fully implementing them? Are some of these laws in conflict? Where are we at in terms of actually carrying out the laws, the authorities that you actually have?

One of the things I will ask the witnesses, as you are talking about this—and, again, I read the testimony. This can be very confusing. Way too many acronyms. As you are evaluating and you are answering question in terms of different laws, different initiatives, I would like to get some kind of sense how far we are. Zero, we have not done anything with it; 10, we have it nailed. I am not expecting any 10s, but I would just like some sort of sense as we are going through this—and if you do not provide it, I will chime in and kind of ask that level of assessment.

I do not think there is any doubt that we have made progress in the last 7 years. In multiple hearings on cybersecurity, this has been a real priority of this Committee. I would always ask what is the number one thing we have to do is information sharing and that we pass those laws, we have given liability protection. How well are they being utilized I think is the main question.

I think the last statement I want to make, again, is just the potential turf battles, which I think is indicative of not being able to pass the renaming of NPPD in the last omnibus. I think that is a serious consideration. We need to probe that and find out where those stumbling blocks are. I realize there is always a little bit of a turf battle between the intelligence community (IC), the Department of Defense (DOD), National Security Agency (NSA), and DHS. From my standpoint and I think this Committee's standpoint, we just recognize DHS is the agency that really has the best capability of dealing with the private sector, and the threats that face our national security, really a great deal of them deal with the private sector, whether it is our financial system, whether it is our electrical grid system, those types of things. I cannot think of a better Department within government to be that focal point and do all those things.

Again, this is very serious. I was telling the witnesses before the hearing, when I talk to young people, either in their last couple of years of high school or early in college, and they are contemplating what they want to do with their lives, what kind of degree program, I always say, "Listen, if you want to get a job and a well-paying job that is going to be around for your working career, check out computer science with a concentration in cybersecurity, and you are going to be pretty well positioned."

I appreciate the witnesses being here. This is a priority of this Committee. It is a pervasive problem. It is not going away. We have got to make continuous improvement as best we can.

With that, I will turn it over to our Ranking Member, Senator McCaskill.

## OPENING STATEMENT OF SENATOR MCCASKILL[1]

Senator MCCASKILL. Thank you Mr. Chairman. I appreciate you holding this hearing.

Hardly a week goes by without some type of cyber incident dominating the headlines. In the United States and the world, as we become more digitally connected, I suspect that trend will only continue and heighten over time.

Our government is a lot older than the Internet, so we have had to retrofit technology into existing government structures. But unlike a lot of issues that naturally fit into a single department or agency, cybersecurity and data protection affect all aspects of government. In the last few years, however, Congress, and in particular this Committee, as the Chairman has just outlined, has made a great deal of progress enhancing the Federal Government's ability to track and improve its cybersecurity.

We codified the Department of Homeland Security to coordinate the operational security of Federal systems. That included designating DHS as the hub for information sharing, running the intrusion prevention and detection programs that are now mandated throughout Federal departments, leading asset response activities, and coordinating the protection of critical infrastructure. When necessary, DHS also has the unique authority to direct another agency to take certain steps to protect its systems.

While every department and agency is ultimately in charge of protecting its own systems, Congress has done a lot to make DHS the primary cyber coordinator for the civilian Federal Government. This hearing is an opportunity to assess how DHS is using those authorities and if these tools are measurably improving the agencies' awareness and security.

As I mentioned, part of DHS' responsibilities also include coordinating critical infrastructure protection, but the majority of critical infrastructure is not federally owned or operated. This is certainly the case with election systems, which are owned and operated by State and local governments.

We all know that the intelligence community assessed with high confidence that Russia launched a campaign to influence the 2016 election, part of which aimed to undermine the public faith in the U.S. democratic process. There is no question that Russia has had a clear plan to break the backbone of democracies wherever they exist. A component of that operation included attempts to hack into voter registration systems.

In the months before the election, DHS stepped up and offered cyber assistance to States that wanted help. In the aftermath of the election, DHS designated election infrastructure as critical infrastructure, which enabled interested States and localities to jump toward the front of the line to receive help.

[1] The prepared statement of Senator McCaskill appears in the Appendix on page 52.

In the roughly 2 years since this issue appeared on the radar of States and the Federal Government, DHS has made progress building relationships with election officials and associated organizations throughout the country and in helping interested States and localities assess and improve the security of their voting systems. There have certainly been some bumps in the road, but I think DHS is on the right track. That said, I have serious reservations about our level of preparedness. Just last week, DHS Secretary Nielsen declined to express confidence in the country's election security, admitting only that there is increased awareness of the threat. That is very troubling.

Beyond that, I am concerned that this Administration has only been treating the symptoms of Russia's interference. U.S. policy toward Russia has been uneven at best, and at worst, I worry that we have not done anything to actually change Russian behavior and stop them from trying to undermine our institutions, especially the institution of democracy.

I look forward to hearing our distinguished witnesses' assessments of our election security and our cybersecurity and how we can continue to improve it in the future.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator McCaskill.

It is the tradition of this Committee to swear in witnesses, so if you will all stand and raise your right hand. Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Ms. MANFRA. I do.

Mr. WILSHUSEN. I do.

Mr. ROSENBACH. I do.

Chairman JOHNSON. Please be seated.

Our first witness is Jeanette Manfra. Ms. Manfra currently serves at the Department of Homeland Security at the Assistant Secretary of the National Protection and Programs Directorate, Office of Cybersecurity and Communications. Ms. Manfra.

## TESTIMONY OF JEANETTE MANFRA,[1] ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. MANFRA. Thank you, sir. Chairman Johnson, Ranking Member McCaskill, and Members of the Committee, thank you for today's opportunity to discuss the Department of Homeland Security's ongoing efforts to reduce and mitigate cybersecurity risks. Safeguarding and securing cyberspace is a core homeland security mission.

For the last decade, I have worked to advance the Department's cybersecurity and critical infrastructure mission. I have personally witnessed the commitment, dedication, and tireless efforts of the men and women at DHS. As cyber threats have evolved in times of calm and in times of crisis, these employees have never wavered in their duty to protect our homeland, and I am proud to serve

[1] The prepared statement of Ms. Manfra appears in the Appendix on page 55.

alongside them as we work to address these important and sometimes complicated national security issues.

On behalf of our workforce and our leadership, I want to thank this Committee for advancing legislation over the last few years that have strengthened our authorities and enabled us to better protect Federal networks and critical infrastructure. Now, as the Chairman mentioned, we must move to the next step: to create the Cybersecurity and Infrastructure Security Agency at DHS, which would see our organization, the National Protection and Programs Directorate, become a new agency.

This change reflects the important work we carry out every day on behalf of the American people to safeguard and secure our critical infrastructure. We strongly support this much needed effort and urge quick action by Congress to pass this law.

Malicious cyber operations remain one of the most significant strategic threats for the United States, holding our national security, economic prosperity, and public health and safety at risk. Over the past year, network defenders have seen the threat landscape grow more crowded, active, and dangerous. One single breach at Equifax and cyber criminals resulted in the online exposure of sensitive personal information belonging to nearly half of all Americans. North Korea's WannaCry ransomware spread to more than 150 countries, paralyzing industries from health care to hospitality. The Russian military-sponsored NotPetya attack was the most destructive and costly cyber attack in history causing billions of dollars in damage across Europe, Asia, and the Americas.

We have taken steps to empower public and private partners to defend against many of these threats by publicly attributing State-sponsored activity, issuing technical indicators, and providing mitigation guidance. Since June 2017, DHS and the Federal Bureau of Investigation (FBI) have published eight technical alerts and malware reports to provide details on the malicious cyber tools of the North Korean Government.

We have also published technical details and alerts regarding Russian-sponsored cyber activity, including operations that targeted U.S. Government and business in the energy, nuclear, water, aviation, and critical manufacturing sectors. These actors also collected information pertaining to industrial control systems.

Last week, DHS joined our colleagues at the FBI and the United Kingdom's National Cybersecurity Center to publish the first international joint alert, which included details and mitigation guidance regarding worldwide cyber exploitation of network infrastructure devices such as routers. With high confidence, we assessed that Russian State-sponsored cyber actors are using compromised routers to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations.

DHS is also working to enhance cyber threat information sharing across the globe to stop incidents before they start. These actions help businesses and government agencies protect their systems and quickly recover should such an attack occur. While in many cases our defenses have been successful in mitigating these threats, we must continue to work to ensure our cyber defenses keep pace with technological change and evolving risks.

I want to assure this Committee that DHS is embracing our statutory responsibility to administer the implementation of Federal agency cybersecurity policies and practices. This Committee played a key role in championing the passage of the Federal Information Security Modernization Act (FISMA) 2014, which provided the Secretary of Homeland Security the authority to develop and oversee implementation of binding operational directives (BOD) to agencies. We have issued a total of six binding operational directives, all of which are now public.

I will discuss one of them, which was the very first BOD that we issued, and I am happy to answer any questions on others. But as an example, the first BOD we issued was around reducing the time to patch known critical vulnerabilities. When we issued this binding operational directive, we were not at an industry standard of time to path being less than 30 days. After we issued this binding operational directive and provided repeated reports to agencies, we are now consistently reducing the time to patch to less than 30 days. In addition to our efforts to protect government networks, we are focused on how government and industry work together to protect the Nation's critical infrastructure.

Before closing, I want to address an issue that I know concerns many in this Congress and among the American public. As Secretary Nielsen said last week, 2 years ago the Russian Government launched a brazen, multifaceted influence campaign aimed at undermining public faith in our democratic process generally and our election specifically. That campaign involved cyber espionage, public disclosure of stolen data, cyber intrusions into State and local voter registration systems, online propaganda, and more. We cannot let it happen again, and that is why DHS has adopted an aggressive posture for helping to defend our election infrastructure.

We are leading the interagency effort to provide voluntary assistance to State and local officials but, more importantly, to help them understand the risk and ensure that when the government has information of value to them that we get it to them.

We will continue to coordinate and collaborate and support State and local officials during the 2018 elections. But cyber actors can come from anywhere, internationally or within the borders, and we are committed to ensuring a coordinated response from DHS to plan for, prepare, and mitigate risk to election infrastructure.

Thank you, and I look forward to your questions regarding our efforts to enhance the Nation's cybersecurity.

Chairman JOHNSON. Thank you, Ms. Manfra.

Our next witness is Greg Wilshusen. Mr. Wilshusen currently served as Director of Information Security Issues at the U.S. Government Accountability Office (GAO). Mr. Wilshusen.

## TESTIMONY OF GREGORY C. WILSHUSEN,[1] DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Johnson, Ranking Member McCaskill, and Members of the Committee, thank you for the opportunity to testify at today's hearing. At your request I will discuss our work related to Federal programs implemented by DHS that are intended to improve the cybersecurity networks and systems supporting Federal operations and our Nation's critical infrastructure.

Before I do, if I may, I would like to recognize several members of my team who were instrumental in preparing my statement and the work underpinning it. With me today are Tammi Kalugdan and Di'Mond Spencer, who are seated right behind me. In addition, Larry Crosland, David Plocher, Kush Malhotra, and Priscilla Smith also made key contributions.

Mr. Chairman, Ranking Member McCaskill, consistent with the statutory authorities, DHS has made important progress implementing programs and activities that are intended to protect Federal and private sector networks and systems. For example, the Department has provided limited intrusion detection and prevention capabilities to entities across the Federal Government. It has also issued cybersecurity-related binding operational directives to Federal agencies, has served as the Federal-civilian interface for sharing cybersecurity-related information with Federal and non-Federal entities, and promoted the use of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, and partially assessed its cybersecurity workforce. However, DHS needs to take additional actions to assure that it successfully mitigates cybersecurity risk.

First, DHS needs to enhance the capabilities of the National Cybersecurity Protection System (NCPS). In 2016, we reported that NCPS had provided the Department with only a limited ability to detect and prevent potentially malicious activity entering and exiting computer networks of Federal agencies. DHS also had not developed much of the planned functionality of the system's information-sharing capability.

Second, DHS needs to evaluate the activities of the National Cybersecurity and Communications Integration Center (NCCIC) more completely. In 2017, we reported that the extent to which NCCIC had performed its required functions in accordance with statutorily defined implementing procedures was unclear because the center had not established metrics and methods for which to evaluate its performance.

We also identified several impediments to the center performing its functions more efficiently, such as the lack of a centralized system for tracking security incidents and not maintaining current contact information for all owners and operators of the most critical cyber-dependant infrastructure assets.

A third activity is that DHS needs to better measure the effectiveness of its cyber risk mitigation activities with private sector partners. In fiscal years (FY) 2016 and 2018, we reported that in

[1] The prepared statement of Mr. Wilshusen appears in the Appendix on page 64.

its role as the lead or co-lead Federal agency for collaborating with partners in 10 critical infrastructure sectors, DHS had not developed metrics to measure and report on the effectiveness of its cyber risk mitigation activities, including activities promoting and assessing private sector adoption of the NIST Cybersecurity Framework or on the cybersecurity posture of those sectors.

Fourth, DHS needs to identify all of its cybersecurity workforce positions and critical skill requirements. In 2018, we reported that the Department had taken steps to assess its cybersecurity workforce; however, it had not identified all of its positions or its critical skill requirements.

Since fiscal year 2016, we have made 29 recommendations to DHS to enhance the capabilities of NCPS, establish metrics and methods for evaluating its performance, and fully assessing its cybersecurity workforce, among other things. The Department generally concurred with these recommendations. As of this month, most of the recommendations remain open, and we are working with DHS to close the recommendations as they are implemented.

Chairman Johnson, Ranking Member McCaskill, this concludes my opening statement. I would be happy to answer your questions.

Chairman JOHNSON. Thank you.

Our final witness is Eric Rosenbach. Mr. Rosenbach is the co-director at Harvard University's Belfer Center for Science and International Affairs. Mr. Rosenbach also previously served as the Deputy Assistant Secretary of Defense for Cyber Policy. Mr. Rosenbach.

## TESTIMONY OF THE HONORABLE ERIC ROSENBACH,[1] CO-DIRECTOR, BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, JOHN F. KENNEDY SCHOOL OF GOVERNMENT, HARVARD UNIVERSITY

Mr. ROSENBACH. Chairman Johnson, Ranking Member McCaskill, other distinguished Members, thank you for calling today's hearing on mitigating America's cyber risk and for the invitation to testify. Thank you also to your hardworking staff who do everything to put a hearing like this together.

Just for a moment, imagine you are watching a science fiction thriller about war in the information age. During the opening scenes of this movie, sophisticated ransomware shuts down the government of a major city for more than a week. A different type of weaponized ransomware, previously deployed by North Korean cyber operators, hits the aircraft production lines at a major aerospace company. Later, the Department of Homeland Security reveals that Russian cyber operatives have compromised important aspects of the Internet's routing infrastructure, and as the plot thickens in this movie, the intelligence community confirms that Russian military intelligence operatives have placed the same malware they used to take down the Ukrainian power grid twice throughout the energy infrastructure in the United States. As the candidates in this movie approach their midterm elections, all of the actors playing experts agree that the risk of Russian cyber and information attacks against election systems is imminent.

[1] The prepared statement of Mr. Rosenbach appears in the Appendix on page 85.

Sitting in the movie theater watching all this unfold, you would probably scream to yourself, “Why are they just sitting there watching all of this happen?” But as you know, all those events are real, and they happened within the last several weeks.

Against this stark reality, America must come together to build real capability and take real actions to address these threats. This hearing and the Committee’s framing of the problem we face as one of managing cyber risk is important. We will not eliminate cyber threats to America, but we can mitigate them. To manage cyber risk, the government must lead a whole-of-nation effort in three specific areas: first, to bolster our domestic capabilities for defense; second, to develop precise and legal offensive cyber capabilities to disrupt cyber and information attacks at their source; and, finally, adopt a clear, public deterrence posture.

For the purposes of my oral statement, I will just hit on some of the key aspects of that first area.

Cyber risk affects all corners of our economy and society. Congress can do more to incentivize the private sector to act. In particular, Congress should: mandate that critical infrastructure providers adopt the NIST Cybersecurity Framework; establish baseline standards for the manufacturers and distributors of the “Internet of things (IOT),” and these devices include things such as home routers, security systems, and thermostats, all of those IOT devices; and, very importantly, ensure that online platforms—primarily Facebook and Twitter—are not used as the tools for foreign adversary information operations.

Organizations outside government must also play a role in protecting the Nation from cyber attack. The Defending Digital Democracy Project that I co-lead up at Belfer Center at the Harvard Kennedy School, along with Robby Mook and Matt Rhoades, works very closely with States to improve their ability to mitigate cyber risk to our election systems. It is clear from our work with the States that they take this risk very seriously. But the States simply are not equipped to face the pointy end of the spear of cyber attacks from nation-state adversaries who are spending billions of dollars and dedicating thousands of cyber operators to advance their national interests.

Our research and work also found that under the leadership of Secretary Nielsen, Under Secretary Krebs, and Assistant Secretary Manfra, DHS has improved support to the States. We also saw that the Department’s efforts to provide real capability are important. Cybersecurity scans and risk assessments to the States have been very productive to help mitigate risk, and Congress should continue to support these.

Furthermore, Congress should support the development of a DHS cybersecurity capability and provide robust resources and authorities for an operationally focused cybersecurity agency. This is more than bureaucratic box-shuffling. The Nation needs an expert-level organization that provides critical infrastructure operators with the support that could make a real difference in mitigating the risk of foreign cyber attack.

When it comes down to protecting elections and critical infrastructure, State governments should also look very closely at strengthening the role that the National Guard and State-run fusion centers play in election-related threat information sharing. This potent combination will provide an important hub for sharing threat intelligence and cybersecurity capability.

Thank you again for the opportunity to testify. I submit my formal testimony for the record and look forward to answering any questions you have.

Chairman JOHNSON. Thank you, Mr. Rosenbach. I will defer my questioning until the very end to be respectful of Members' time. I will go to Senator McCaskill.

Senator MCCASKILL. Great. Let me start with the 21 States. Assistant Secretary Manfra, you testified before the Senate Intelligence Committee that 21 States were affected by Russia's cyber activity. But my understanding is that number only reflects the States where there were censors or tools in place to capture the Russian activity. Is that correct?

Ms. MANFRA. Yes, the 21 States references the visibility that we had, whether that was the intelligence community or the censors of Russian targeting of State infrastructure related to elections.

Senator MCCASKILL. But have we checked with the remaining States to determine whether they had tools in place that would have captured that activity?

Ms. MANFRA. Many of the States did have some capability that could have captured it.

Senator MCCASKILL. How many?

Ms. MANFRA. I do not know off the top of my head, ma'am.

Senator MCCASKILL. That would be something we would want to know, because I think the American people have been misled here, because it is my understanding that a number of the States do not have the tools to capture that activity, so we really have no idea how many States Russia tried to hack.

Ms. MANFRA. That is correct, ma'am, and I think we can assume that the majority of States were probably a target. What we have is the visibility that we had at the time. What I can also say is that we have many more States now who are moving their systems behind those censors that we have deployed via the Multi-State Information Sharing and Analysis Center (MS–ISAC), so we are increasing our visibility.

Senator MCCASKILL. I think the thing that I did not realize until I began really understanding what happened is the impression that was given at the time is that we had knowledge that 21 States were hacked, and the assumption was that the remaining States were not hacked. But, in fact, that is an incorrect assumption.

Ms. MANFRA. Twenty-one States were not hacked, ma'am.

Senator MCCASKILL. There was an attempt to target 21 States that we know of by Russia in terms of their voter registration systems.

Ms. MANFRA. There was targeting via scanning, which is a common activity on the Internet. The reason we are concerned is because of where it was coming from, and the actual attempts to get into systems which was a much smaller number. But, yes, ma'am, you are correct. We only had the visibility that we had, and I believe I have been clear about that as I have discussed it. But, yes, how the media reports it I cannot control.

Senator MCCASKILL. I sympathize with you there. We cannot control how it gets reported. But I want to make clear today on the record that it is likely that all 50 States were likely affected and that States that were not on that list were less vulnerable. But that is simply not true. States that were not on that list, in fact, might be more vulnerable.

Ms. MANFRA. I would not necessarily make a connection between vulnerability in the States as to whether they were targeted. Every organization is scanned a lot, sometimes thousands of times a day. What we were trying to differentiate between is what we saw, very concerning activity from known suspicious servers in this case that, as far as the visibility we had, and they were targeting to look for vulnerabilities. Most of the States that we had visibility into did block it.

Your overall point is correct, ma'am. I just do not want to make this——

Senator MCCASKILL. Yes, I just think we all kind of go, OK, 21 States, they were not successful, OK, good, not a problem, when in reality I think the more accurate pronouncement would have been probably tried all the States, these were the States we could see they were trying.

Ms. MANFRA. That is correct. Fact-based, 21 States, but we can absolutely make the assumption that more would have been targeted.

Senator MCCASKILL. OK. How many people does DHS have working full-time focused on election security and election infrastructure?

Ms. MANFRA. Ma'am, I will have to come back to you with the exact number, but the Election Task Force comprises about 10 to 15 people.

Senator MCCASKILL. They do this full-time, nothing else?

Ms. MANFRA. The majority of them are doing this full-time, and then we have it prioritized for all the other teams throughout my thousand-person organization.

Senator MCCASKILL. OK. I would like the number of how many people are working full-time on election security and infrastructure security. Is it someone's job to just focus on election security?

Ms. MANFRA. Yes, Senator. We have a senior person who has been working in my organization for a long time. His job 100 percent of the time is running the Election Task Force.

Senator MCCASKILL. OK. Seventeen States have requested risk assessment?

Ms. MANFRA. Yes, ma'am.

Senator MCCASKILL. Can you give us insight as to why States are declining the assistance?

Ms. MANFRA. It varies. Many of the States we talk to already have this type of service from the private sector, which we enthusiastically endorse. These are services that are provided by the market.

Senator MCCASKILL. They are paying for that?

Ms. MANFRA. Yes.

Senator MCCASKILL. Yours is free?

Ms. MANFRA. Yes, ma'am.

Senator MCCASKILL. You will not tell me whether my State is one of those?

Ms. MANFRA. Missouri is working with us. I would have to direct you to Missouri for more details on what they are doing.

Senator MCCASKILL. At DHS' request Congress included $26 million for the Department's election work in the omnibus. Mr. Rosenbach, you are an outside observer of the work DHS has been doing, and you have been visiting election officials throughout the country. Every time I ask DHS if they need more resources, they have to say they are doing their work with the resources they have.

As an outside observer, do you think we need to scale up the DHS efforts? Or is it right-sized?

Mr. ROSENBACH. Yes, ma'am, it is always easier when you are on the outside to answer money questions, but I would say I am sure that Secretary Manfra would benefit from additional resources, both financial and personnel. Making sure that they are good and capable is always a challenge. But this is one of the most important national security issues facing the country right now. Twenty-six million dollars is not very much money in the——

Senator MCCASKILL. It is not very much money. How many people are waiting right now for an assessment that have not been able to get it yet? How many States, I should say?

Ms. MANFRA. Nobody in the election community is waiting for an assessment. Because we prioritized them, we now have a significant backlog in other critical infrastructure sectors in Federal agencies, but nobody in the election community is waiting.

Senator MCCASKILL. If someone decided tomorrow that they wanted to get this done, you would be able to accommodate that prior to the elections beginning later this year?

Ms. MANFRA. Yes, ma'am.

Senator MCCASKILL. OK. Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator McCaskill.

I am going to take just a couple of minutes to make a point and also ask a question. I was in the September 2016 briefing. Senator Carper was there. Ms. Manfra, you were there. We were briefed about Russian attempts in the election, and it was Secretary Jeh Johnson, it was FBI Director James Comey, and Lisa Monaco, a member of the Obama Administration.

The thrust of that briefing, without providing any classified information, was Russia has attempted this, they have attempted to hack into voter files, but the Administration has this under control, they are in contact with the States, and the main message we want you as Members of Congress, because it is so important in terms of the stability of our democracy to let the public know that we have this covered, and that the election in November will be legitimate.

First of all, is that pretty much an accurate description, Ms. Manfra, of what we were being told as Members in that briefing?

Ms. MANFRA. Yes, sir, my recollection was that the leadership laid out the risk as they saw it, the intelligence as we saw it, but that is a fair conclusion.

Chairman JOHNSON. From my own standpoint, because I heard that they were trying to access voter files, I was not willing to make that statement publicly, but I told the briefers that I am not going to dispute if you go out there and talk about that, because I think there are plenty of controls, a number of things that we can look to indicators in terms of whether voting tallies or an election have actually been affected in some way, shape, or form.

This is a serious issue, no doubt about it, but I think we also have to be very careful not to blow it out of proportion. When I am looking at the problems with cybersecurity, I am far more concerned about attacks into our electrical grid or into our financial system. They could be unbelievably disruptive, and there may not be controls.

We may be playing into Russia's hands, quite honestly. They are achieving exactly what they wanted to achieve, to all of a sudden call into question the legitimacy of the election. We have no control over these things, and this is an enormous problem that threatens our democracy. I just do not think that is the case. I think we need to take this issue seriously. We need to push back. We have obviously imposed sanctions on Russia, but we need to keep all these things in perspective and really focus on, in terms of DHS' time, you always have to prioritize things, the things that could really bring down this country. That from my standpoint is the other aspect of our critical infrastructure.

That is my statement and my questions. Senator Hassan.

## OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you very much, and I thank Senator Peters for deferring to me. I have a vote at 10:45. We have worked it out with collaboration.

Chairman JOHNSON. You guys are moving all over on me.

Senator HASSAN. First of all, welcome to the panel, and as always, I am sorry that we are all in and out at multiple committee hearings.

I wanted to start with a question to you, Ms. Manfra, because I am very concerned about election security. I do think it is the bedrock of our democracy, and I think we have to take it incredibly seriously. As you know, the 2018 election cycle is well underway. Six States have held their primaries, and dozens more will do so in the next couple of weeks.

To this point, has DHS detected any cyber activity targeting election infrastructure by Russia or any other actors during this election season?

Ms. MANFRA. We have not at this time, ma'am.

Senator HASSAN. Thank you. Last week, when Secretary Nielsen was asked whether she had confidence in U.S. election security, she did not provide the assurances that many of us wanted or, frankly, expected to hear from her. Do you have confidence in the security of our Nation's election systems? If not, then why?

Ms. MANFRA. If I may, because I was there when Secretary Nielsen was speaking, what she was trying to convey and what I believe she did convey, which is the same sentiment that I have, is we do not have perfect visibility into every State and local system. What we have confidence in is that DHS is doing everything that we can, that the government is doing everything we can, and that we have greater visibility than we did in 2016. Not to parse words, ma'am, but to be clear, in no sector would I ever say I have complete confidence that nothing will ever happen, because that would be a foolhardy statement, I believe.

Senator HASSAN. Thank you for that clarification. I would encourage DHS, as many of us have been, to continue to reach out to the States. The States obviously have their own obligations and constitutional responsibilities, and I think intense collaboration is called for every single day as vigilantly and constantly as possible. I thank you for your efforts, and I look forward to hearing and seeing more of the results from those efforts.

I also had a question, Mr. Rosenbach, for you. It is nice to see you again. Last year, you testified before the Commerce Committee on emerging cyber technologies. I serve on that Committee, and we discussed the need to secure the Internet of things at the hearing. You emphasized that the government needs to lead the effort to secure the Internet of things, and I see in your testimony today that you argue for the establishment of baseline security standards for the manufacturers and distributors of these Internet-connected devices.

Given these positions, I want to draw your attention to a bill which I was an early cosponsor of, the Internet of Things Cybersecurity Improvement Act, which was introduced by Senate Intelligence Committee Ranking Member Mark Warner. This bill requires that when the Federal Government purchases an Internet-connected device for government use, the devices must adhere to specific minimum cybersecurity standards as established by the National Institute of Standards and Technology. According to one report, the Federal Government purchases more than $8 billion worth of Internet-connected devices each year.

The idea behind this bill is that the Federal Government as a major purchaser of Internet-connected devices will lead the way on Internet of things security and will push the consumer market to step up its security efforts as well.

Mr. Rosenbach, given your advocacy for minimum standards for Internet of things security, what is your opinion of the approach in Senator Warner's bill as a first step toward achieving the goals you laid out?

Mr. ROSENBACH. Thank you, Senator. I have looked at the bill, and I am a very strong believer in improving the security of the Internet of things. I think you always need to be careful about a regulatory approach, but from my professional perspective, many of the things that you lay out in that bill I think are very strong, and we need to do something in this space given the tremendous growth of devices that are connected to the Internet. Having government use its contracting leverage I think is a good place to start.

Senator HASSAN. Thank you very much. I appreciate that. I will submit my other questions for the record.

Thank you again, Mr. Chair, and Senator Peters for your deference.

Chairman JOHNSON. Senator Peters.

## OPENING STATEMENT OF SENATOR PETERS

Senator PETERS. Thank you, Mr. Chairman. And thank you to the witnesses for your testimony here today.

Well, obviously, as we have been having this discussion about elections and with local governments, I think it leads to the question that I have for you. With the creation of and support of processes to ensure coordination between the Federal entities and State authorities during cyber events, it is certainly essential that we have effective responses. So my question, Ms. Manfra, is: How exactly is the DHS promoting alignment of State cybersecurity plans with the National Cyber Incident Response Plan? And are there barriers to encouraging States or incentivizing States to align these plans?

Ms. MANFRA. Thank you, sir. Great question. We have been working with States for some time, though I have been stepping up those efforts not just for elections but just in general, of how States protect personally identifiable information (PII) that they have access to, which is a tremendous amount of data that is stored on their networks. We are leveraging a lot of the work that we have done on public safety communications around trying to address interoperability challenges to how we might address some of the cybersecurity and having the planning phase be very collaborative and tailored to the State. Every State is very different, whether they have a centralized network approach or not. We are working with the National Governors Association, policy academies, and we have technical assistance capabilities where we can help States organize themselves and develop a plan.

Then there are a few kind of outstanding questions, I would say. We are working with the Federal Emergency Management Agency (FEMA) and the States to think about, from a cyber perspective, what fits in existing emergency management frameworks where we already have a well-defined process for how a Governor, National Guard, or other organizations that we traditionally use as a physical incident, if you will, goes from local to more significant. I believe that we want to leverage that as much as possible, but there are certain scenarios where it is less clear about what is the Governor's role in a certain situation. Is it because the company is headquartered there, for example? But if it is a multinational company, what does that look like?

There are still some outstanding questions, and I believe the States have rightly been pushing to have some of these questions answered so it is clear on what the expectations are, if that answers your question.

Senator PETERS. It does, and you bring up FEMA. That actually leads to my next question here. According to a 2017 National Preparedness Report, while States and territories continue to indicate that cybersecurity is a high priority, most actually rate themselves as lacking proficiency in it than any other core capability. In the past DHS and FEMA have used preparedness grants to drive action toward agreed-upon deficiencies or priorities, as you know. Despite being an allowable expense under a number of preparedness grant programs, spending on cybersecurity-related activity is just a fraction of that spent on other capabilities, even though they rank it so lowly.

My question is: Has there been any consideration with DHS to change grant guidance or selection criteria for any existing State and local preparedness grant programs to push State and local governments to spend money to address what is an admitted lack of proficiency in cybersecurity?

Ms. MANFRA. First, I will speak to the grants question, and then to some other areas where we are working to shore up some of their gaps. I have been working very closely with FEMA, though they are not the only grants that can be leveraged for cybersecurity purposes. We are working broadly within the Federal grant community, but more specifically with FEMA, how can we provide more specific guidance on what we would like to see States buy. Cybersecurity is very broad, sometimes overwhelming, and for organizations to try to figure out how to prioritize their limited resources, they are trying to provide more discrete guidance, working with State and local officials, working with grants administrators to figure out first why are they not using more grant money for this gap and what more specific guidance.

The other area that is a challenge is personnel, and our Scholarship for Service Program, which I think has not been as widely known as it should be—it is called the "CyberCorps: Scholarship for Service," us, the NSA, work with the National Science Foundation to fund scholarships, 2-, 4-, and plus-year scholarships. The only requirement is that they serve in a government agency, meaning State and local governments can benefit from these students coming out of these programs. The government has already paid for the scholarships, and the State and local agencies can benefit.

While I want these personnel as well, because I have just as many challenges, we are working with the States to make sure they are aware of it and have access to these personnel coming out of these programs.

Senator PETERS. You raise the issue of personnel, and that leads to my final question. I want to touch briefly on an effort that I am working on with my colleague Senator Hoeven, and I hope the Committee will take up a bill in our next markup, which is Senate bill 2620, the Federal Cybersecurity Joint Duty Program, which assists the Federal Government in developing an integrated cybersecurity workforce and allows rotation, similarly in the intelligence community as well as in the defense community. All of the witnesses could respond, if you would. In your opinion, would a joint duty program that provides rotational opportunities to cybersecurity employees be beneficial to both cyber employees as well as the Federal Government as a whole? We can start at this end.

Mr. ROSENBACH. Yes, sir, I think this is a great idea. Having worked in the Department of Defense the last 8 years, it would be really important for U.S. Cyber Command (CYBERCOM) people to be able to go help out DHS, learn from DHS as well, along with some of the other agencies. It sounds like a great idea.

Senator PETERS. Great. Thank you.

Mr. WILSHUSEN. I would agree. Anytime you can bring in new, fresh ideas and gain greater perspective on how to secure systems, it is going to be a benefit to all.

Senator PETERS. Great. Thank you.

Ms. MANFRA. Sir, I look forward to working on the specifics of the bill, but generally, we are trying to think differently about the Federal cyber workforce. We cannot meet the demands in the current model, and I absolutely think being able to rotate personnel through agencies under sort of DHS' oversight, if you will, is something that we would be very willing to continue talking to you about.

Senator PETERS. In the remaining time, I have this question. This could also help with hiring and retention. We find that job satisfaction goes up when folks are able to rotate, see other parts of the whole government. Would you agree, in the 5 seconds remaining, the three of you?

Ms. MANFRA. I would agree, and I believe it would also bring more consistency to the level of training, which is something that we are also looking to improve.

Senator PETERS. Great.

Mr. WILSHUSEN. I would also agree with that. We have a similar program, internal to GAO, in terms of rotating auditors among different audit groups, and it helps significantly.

Senator PETERS. Great.

Mr. ROSENBACH. Sir, anytime you can tell a cyber expert that they can go to NSA or CYBERCOM and legally hack the Iranian, North Koreans, or Russians for several years, they are going to stay in the government.

Senator PETERS. Great. I am out of time, but I appreciate your answers. Thank you.

Chairman JOHNSON. Let me just quickly follow up. Is a piece of legislation required, or would you have the authority right now to do those rotations?

Ms. MANFRA. I am not a lawyer, nor a personnel expert, so we would have to check on that, sir. I know that we have the ability to do interagency rotations, which we have been exploring, but we can get back to you on the specifics of whether we——

Chairman JOHNSON. Maybe GAO would have some indication of that.

Mr. WILSHUSEN. Actually, I do not sir, but I can get back to you on that.

Chairman JOHNSON. OK.

Mr. ROSENBACH. Sir, all I know is during the 7-years I was in DOD, it was very rare to see something like that happen.

Chairman JOHNSON. Never happened?

Mr. ROSENBACH. Maybe authorities, maybe strong leadership, but something to facilitate it would be helpful.

Senator PETERS. My understanding is that it does require legislation to be able to move between these agencies, and so that is why——

Chairman JOHNSON. OK. We will work with you on that.

Senator PETERS. Great.

Chairman JOHNSON. Thanks. Senator Lankford.

## OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thank you, Mr. Chairman. Thank you all for being here as well. Let me talk through a couple of things.

Ms. Manfra, tell me about lessons learned on Kaspersky. We had a long conversation about supply chain. DHS has this responsibility to be able to help work with GSA and whoever it might be to be able to help get products out there and to be able to manage them. Then once we find out we have a product that has a problem, trying to be able to get it back out. Let us talk big picture. What are the lessons learned so far on that, including the status? Is every agency clean of Kaspersky Lab's products at this point? What have we learned from it?

Ms. MANFRA. I will answer the second first. Yes, 100 percent of agencies are in compliance with the BOD.

Lessons learned? I guess I will come from me personally in our organization. Maybe others in the government already knew some of these, but lessons learned I would say is that we need to modernize how the government thinks about third-party risk, and procurement officials having access to information that is necessary for them to make appropriate risk decisions; mission owners, network owners, and system owners thinking about supply chain risk and having guidance and better connecting our intelligence community with the acquisition community. Those are some of the high-level lessons, and we are implementing based on that.

Senator LANKFORD. Who provides that guidance to them? Is that something each agency is responsible for or DHS is responsible for getting that to the agencies, then they get it down? How does that work?

Ms. MANFRA. The Office of Management and Budget (OMB) is responsible for overall acquisition guidance and the regulations around it, and then there are statutes, of course, that govern it. I believe DHS has a responsibility to provide that risk picture for government, either agencies individually or as an enterprise. We have been working very closely with OMB and other organizations on how do we improve that guidance and how do we ensure that DHS has a strong role in that process.

Senator LANKFORD. How does this become an issue where DHS is going to help us with supply chain without everyone having to play "Mother, May I?" with your office every time they want to get a new printer to say, hey, this printer has this new Internet of things connection to it, and it has something else additional, we want to be able to get this, and suddenly you have to do a check. How are we developing standards and communicating that down rather than having to check each item?

Ms. MANFRA. At a highest level, the government needs to have a framework for how we think about supply chain risk, not just for the government but also so the private sector can understand how we think about supply chain risk, and we are working on that. Then it is about if there are hurdles that are preventing us from achieving some of these, whether that is through policy or regulation or statute, then we need to figure out what those are and remove those obstacles, which are also working through that process. It is quite complicated, as you may know, the acquisition process.

The last piece is providing more guidance. These are the types of things that you should ask. This is how you should run your contracting process. These are the types of terms that you should put in your contracts if you are procuring a product or a service. Our plan is only for a very limited set, what we would call the "high-value assets," who will actually go through a more thorough process where we would actually review a more thorough supply chain due diligence, if you will, not every single system in the government.

Senator LANKFORD. But many of the systems are connected to us.

Ms. MANFRA. Yes.

Senator LANKFORD. They become vulnerability points, whether that be a new thermostat that they install that is connected, or whether that be a new refrigerator they put in that has something to be able to connect to the WiFi on it, or the Coke machine that is down the hall.

Ms. MANFRA. Right.

Senator LANKFORD. All these things have vulnerabilities. What is the process of helping agencies understand when you add something that has Internet of things on it, you are adding a vulnerability to your system once you connect it to your main communication?

Ms. MANFRA. Getting in the Internet of things, I think that is—and Eric Rosenbach mentioned this as well. I believe that we need more industry-driven standards for Internet of things diversity. If you look back at, say, Energy Star, which we have done some research on that, first, you had to have this kind of industry-driven standard, and then the government using its procurement authority to mandate, OK, we are only going to buy Energy Star products. Right now that does not really exist in the Internet of things, so it would have to be guidance of—again, it would go back to a higher-level framework. Where is this produced? Do you have insight into the code where it came from? Do you understand where it was manufactured? Which right now is hard.

Senator LANKFORD. Can the password be changed?

Ms. MANFRA. Can the password be changed? Right now that is quite cumbersome for agencies, but at the moment that is all we have, so that is the type of guidance we will be putting out.

Senator LANKFORD. OK. That is one we will look forward to just following up on to be able to see where that goes, because this is going to quickly accelerate in a hurry. The more products we have out there that the password cannot be changed and updated, we have a default access point into our systems.

Tell me about this wonderful new Cybersecurity and Infrastructure Security Agency. Why do we need to stand up a new agency? What is it that you are seeing that would say we cannot do it under existing structures, we are going to need a whole new structure to be able to accomplish that?

Ms. MANFRA. What we are looking at doing is transitioning the National Protection and Programs Directorate, which is currently a headquarters agency, and we do not have to go into the details, but there is actually administrative reasons why it would benefit the Department to stand us up as an operational agency.

There is some minor restructuring that we would like to do, but the biggest thing that we are asking for is the change in the name, which does require an act of Congress to do that. I know it is hard sometimes maybe for people to understand why this is so important, but it is very hard to go out and try to market our organization, which is purely dependent upon voluntary partnerships and critical infrastructure with a name like the "National Protection and Programs Directorate." It is also a morale issue for our workforce. They do not have a name that sort of reflects what they do.

Senator LANKFORD. Is this an increase in staffing? Is this combining other offices? Or is it just switching that one office and switching the name and some of the placement of it? What else will you need?

Ms. MANFRA. What we are asking for does not increase staff or resources in this legislation. We are asking for just the name change and the authority to make some restructuring, just to make us more efficient internally.

Senator LANKFORD. OK. Thank you.

Mr. WILSHUSEN. Senator Lankford, if I could also just add a comment. GAO went through a similar name change back in the year 2000. Our previous name was "General Accounting Office," and I can personally speak to the fact that when I went out on recruiting efforts and trips, people would see "General Accounting Office" and just keep walking by. I would have to go out from behind my booth and tell them, "No. We do much more than that." It really does have an impact if your name reflects your mission, and it creates esprit de corps as well as helping to generate interest in your work.

Senator LANKFORD. That is great. Thank you.

Chairman JOHNSON. I cannot imagine anybody walking by something dealing with accounting, but—— [Laughter.] Senator Harris.

## OPENING STATEMENT OF SENATOR HARRIS

Senator HARRIS. Thank you.

Mr. Rosenbach, as you know, Congress recently added $380 million to the omnibus to upgrade States' election technology. As I think you know, the omnibus allocates and prioritizes the money going to States based on the population of the State versus the need the State has to actually upgrade its technology. As you know, we have the Secure Elections Act. Senator Lankford and I and some of our colleagues are working on that to provide some standards for States on how they are going to actually be equipped to meet the challenges that we now know we face.

What are your thoughts about whether or not we should be prioritizing the funding to States and how those priorities should be outlined in a way that actually will achieve the goal, which is that all States will have secure elections?

Mr. ROSENBACH. Thank you, ma'am. An interesting story for you is we were holding a national-level tabletop exercise with 39 States up at Harvard the day the States were getting the news about how much money they would receive, and so they found out, they were happy. But they were unsure even with those State election officials how to best spend the money.

Senator HARRIS. Right.

Mr. ROSENBACH. I think it establishes what your main point is. I would say that I think the Secure Elections Act is excellent, it is bipartisan, it gives guidance on information sharing, a little bit of litigation protection, which is good, and a process for grant provisions, which goes on.

I think for the States, though, first of all, you would want to be very careful about any strict Federal guidance about how to spend it because it may be counterproductive in the relationship that DHS in particular right now is building. They have done a good job over the last year rebuilding trust with the States, and their autonomy is important.

But I think there should be some general guidelines or a framework, maybe a NIST-like framework in which trusted parties work with States to help them decide the best way to allocate that money so that it has maximum effectiveness.

Senator HARRIS. As you can probably tell from my question, I am speaking against perhaps what would seem to be the better interests of a large State, but I do know that being large should not necessarily because the priority. The priority should, I believe, be based on need as well.

Mr. ROSENBACH. Yes, ma'am.

Senator HARRIS. Looking at the priorities from that perspective. You do support that?

Mr. ROSENBACH. Yes, ma'am. I totally agree, and here is why: Some States are much better off when it comes to protecting their election systems, and, remember, the Russians in particular do not have to attack every State. They will go to the weakest link. It does not have to be a prominent State or a battleground State. All they have to do is undermine trust in the system and confidence in the outcome, and that could be someplace that is very weak. We should try to address it from that perspective rather than a thin smear everywhere.

Senator HARRIS. Well said. As we know, that was their goal, to undermine Americans' confidence in their democracy.

Secretary Manfra, I saw you nodding your head. If you would like to add anything to the comments?

Ms. MANFRA. Yes, ma'am. I would say—first of all, I just want to thank you and Senator Lankford for your leadership on the legislation, and I think that we like to take a risk-based approach to everything that we do. I do think population can be a part of that risk-based approach, and we are working with the Government Coordinating Council (GCC), which is a name for the group of bipartisan representatives, Secretaries of State, as well as local election officials and other election experts. We are working on some guidance that can assist in how they spend that money. But I agree that a risk-based approach is usually a good way to go for spending grant dollars.

Senator HARRIS. Thank you.

Mr. Rosenbach, what are your thoughts about what we need, if we need any more funding beyond that $380 million? Do you have some thoughts about that?

Mr. ROSENBACH. if you look back in history and the reason why there are vulnerabilities, the Help Americans Vote Act allocated money that brought about some of this technology, but then the funding tail after that was dry. Remember, in cybersecurity, in all operations——

Senator HARRIS. Or just nonexistent.

Mr. ROSENBACH. Right, it was dry. There was no follow. What we do not want is one big bump of money now and then nothing in the 5 years after that. Cybersecurity is about continually mitigating risk and patching, so you need some reliable funding stream so the States know that they can patch these systems, that they have a pool of money to go to to keep it secure over the long run.

Senator HARRIS. That is a great point because by the very nature of technology, we know that it is constantly evolving. There is something that is very static about technology, which is that it is dynamic. It is constantly changing.

I want to talk with you about the Election Assistance Commission (EAC). Do you know if they have anyone working in-house who can provide technical expertise to inform their best practices, like a chief technologist? Do you know if they have one? Because I am not clear about that.

Mr. ROSENBACH. In our project at the Kennedy School, we have been working really closely with EAC. Matt Masterson, when he was there, was amazing to work with, and he is now at DHS, which I think is good for the country. They have some technical expertise, but, that is not their strong suit. There would be additional help needed there.

Senator HARRIS. In your opinion, would it be beneficial to national security, to elections, and protecting that critical infrastructure, that they would have a chief technologist position there?

Mr. ROSENBACH. A lot of elections nowadays revolve around technology in one way or another, so almost all organization nowadays have some type of chief technology officer. That makes good sense to me.

Senator HARRIS. Do any of the other panelists have a thought about this?

Ms. MANFRA. I would say I agree with Eric. Most organizations that deal with technology benefit from having a qualified chief technologist. The National Institute for Standards and Technology has long supported EAC in the development of the voluntary voting systems guidelines to include some of the technical—we have been assisting, but, yes, I would say it would benefit from that.

Senator HARRIS. Thank you.

Do you have any thoughts?

Mr. WILSHUSEN. I was just going to say that the EAC is presently updating the standards now. I think the guidelines, I should say, are probably 10 or 15 years old. The EAC is reaching out to a number of different groups and experts as they go through that. My understanding is that the EAC expects to issue those updated guidelines later this year.

Senator HARRIS. Hopefully, they also commit themselves to appointing and having a chief technologist.

I have just one final question, Mr. Chairman. When I was Attorney General (AG) of California, we had a law that now I believe all 50 States have which is basically a data breach notification law, requiring, for example, corporations that experience a data breach that affects more than 500 Californians, the case in California, that they had a responsibility to report that data breach to the State Department of Justice, the Attorney General.

Do any of you know, because it is my understanding that there is no such requirement for Federal agencies, that if they experience a data breach they have a responsibility to report that to another body so that the consumer—and that would be the taxpayer—is aware that there has been such a data breach. For the sake of brevity, do you think it would be a good idea to have such a law? You can just give me a yes or no answer. Mr. Rosenbach.

Mr. ROSENBACH. Yes, ma'am. If you talk to private sector people, they spend an immense amount of time of legal hours and cost trying to figure out the patchwork quilt of data breach notification laws in the United States.

Senator HARRIS. OK. What is your thought?

Mr. WILSHUSEN. You mean for the Federal Government; to have Federal agencies report breaches?

Senator HARRIS. Correct.

Mr. WILSHUSEN. Agencies are supposed to be reporting to the U.S. Computer Emergency Readiness Team (US–CERT) when they have security incidents, and if they have a major security breach, they are also supposed to report to Congress under the Federal Information Security Modernization Act of 2014.

Senator HARRIS. Do you believe that is happening?

Mr. WILSHUSEN. I think they are reporting incidents to US–CERT. I do not know if they are reporting all of them, though.

Senator HARRIS. Or if they are reporting to Congress.

Mr. WILSHUSEN. I think they reported like five or so. I think the bar for reporting what is a significant or major information security incident can be pretty high, or at least interpreted to be high.

Ms. MANFRA. Yes, ma'am, they are required to report to us as well as their oversight committees. I can say that the reporting has increased. We are also deploying more capability so we can independently see whether we have something. But the reporting has increased to the Department, and in many cases we have worked with agencies on assisting with communications to Congress. I know that, at least in my perception, that is increasing as a result of that. But, of course, there is always—and the private sector has the same challenge. What is a significant incident? Particularly if it is not clear, if it is not a data breach, for example, where you can count the number of PII that has been lost.

Senator HARRIS. Mr. Chairman, thank you. I appreciate the time.

Chairman JOHNSON. While we are on the topic, in these previous hearings I talked about the priority, what we had to do, we had to do something. First was information sharing. Then it was data breach notification. I thought, well, that ought to be a no-brainer. But, over the years, I have come to understand how unbelievably complex that is.

While we are on the subject, Ms. Manfra, you can just talk about it is difficult to define, you are not exactly sure if you have been breached. Just talk about the complexity and why we have not been able to come up with a national standard on that to preempt all these State laws, which makes it very difficult for anybody to comply.

Ms. MANFRA. Absolutely. The patchwork of data breach notification requirements by the States can be challenging. My experience has been that it is more about the time, because you do not always know right away how serious it is, and you do not always know who is doing it to you, which has a big impact, and whether you call this serious or not. It takes longer than most people actually appreciate to understand the scope of the incident. It is the threshold we have worked with in the government, we have created an incident severity scheme now that has been used for a couple of years. I think people generally understand this is why something should rise to the level, and we do our best to brief Congress. But it really comes down to that timing, as I understand it. What is the right amount of time to give a company or an agency to figure out what is really going on before they have to notify the public, the victims, or Congress.

Chairman JOHNSON. Part of the problem, when you have been breached, sometimes those malign actors are on your system for hundreds of days before you even notice, and then you have to start doing the attribution. You have to do the forensics to find out is there really a breach or is this just a computer bug or something else. Correct?

Ms. MANFRA. Right.

Chairman JOHNSON. Senator Carper.

## OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Let us talk some more about data breach. About 10 years ago, Roy Blunt and I introduced legislation on data breach. I used the acronym PIN, spoke to how we needed to do a better job protecting our sensitive information; second, investigate laying out expectations for an investigation to proceed; and, finally, notification. The idea of having 50 States going their own way just made no sense to Senator Blunt or me. As it turns out, it made no sense to Senator Nelson, it made no sense to Senator Feinstein, it made no sense to Senator Thune and others as well. We ended up with four committees of jurisdiction on data breach legislation, including this Committee, Judiciary, Commerce, and Intelligence. We all have our different stakeholders and folks that are interested in what we are doing and considering. It has just been——

Chairman JOHNSON. Not a recipe for success, you are saying.

Senator CARPER. If you want to have a good picture of what is not working around here, it is getting data breach legislation enacted. But I am pleased that we are talking about it again today. Senator Blunt and I talked about not long ago.

The idea of inviting a couple of you just to meet with the legislative leaders, Democrat and Republican leaders of these four committees of jurisdiction, and sharing with you what we have offered, and the staff will continue to have discussions at the staff level, but that might be helpful for us actually getting the show on the road. Would you be willing maybe to do that?

Ms. MANFRA. I would be happy to do that, Senator.

Senator CARPER. Oh, good. Thank you. Greg, we might even try to drag you with us as well.

Mr. WILSHUSEN. Absolutely. We have done a couple reviews looking at data breach response as well as cybersecurity incident response. We would be happy to talk about that, too.

Senator CARPER. Great. All right. Thanks so much.

I want to come back to a name change and just to say the name remains the same, and I agree with you, it is time to actually say what you do, and I do not think we are looking to do a whole lot more beyond that, but that would be a big deal. We are all interested in our business in branding, and I think it is understandable why that is important to you.

Jeh Johnson was in town not long ago, and we had a chance to visit, and Ali Mayorkas on a separate visit. We talked about morale within the Department of Homeland Security, and I think if you look at the Federal agencies where we evaluate morale on an annual basis, the agency or the department that had the biggest uptick in morale was the Department of Homeland Security. That is something that the Chairman, the Ranking Member, and myself and others have focused on, and we are very pleased to see that. I believe your point, Madam Secretary, about having an agency that actually says what you do—and Mr. Wilshusen alluded to this as well—makes a whole lot of sense.

One of the things that I like to do as a Senator—and I used to do it as Governor—I like to do customer calls. I call on businesses large and small, schools, hospitals in Delaware, and even outside of Delaware, to see what we can learn from them. We always ask three questions: How are you doing? How are we doing? "We" being Delaware, the State of Delaware, or Congress, our congressional delegation, or the Federal Government. What can we do to help? We asked these questions a lot about 3 or 4 years ago, and folks here to my left were a part of those conversations. Tom Coburn was a part of those conversations. I was a part of those conversations. We said, "What can we do to help?" One of the things you said we could do to help was on the workforce side. We did, I think, a fair amount. Has it helped? What have we done that is helpful? What have you not taken full advantage of what we provided for you legislatively? If you all could take a minute on that workforce, how are we doing? I do not care who answers it. Maybe both of you can.

Mr. WILSHUSEN. We recently issued a report last month on DHS' efforts implementing that Homeland Security Cybersecurity Workforce Assessment Act of 2014 in which it was responsible for identifying all of its cybersecurity positions, assigning codes to those positions based upon the work roles and the work categories, the specialty areas of those positions, and then to identify its critical needs and gaps. We found to a large extent that the Department had not implemented those actions in accordance with the deadlines established in law, but they are working toward it and have taken actions on it.

We also found, even though it was not part of our report, one of the authorities granted to the Department under the Border Patrol Agent Pay Reform Act of 2014——

Senator CARPER. That was the one.

Mr. WILSHUSEN. Right. Even though we were not examining that, we had heard that despite having these authorities to hire new cybersecurity-related personnel, the Department as of at least earlier this year had not really taken advantage of it for 3 or 4 years. But, again, that was really something we heard in passing. It was not a focus of our review. We were just examining the Department's implementation of the Homeland Security Cybersecurity Workforce Assessment Act.

Senator CARPER. Madam Secretary, just briefly, any comments?

Ms. MANFRA. As Greg mentioned, the responsibility for implementing that authority is with the Chief Human Capital Officer of the Department, which is not my organization, but we are working very closely with them. I think she has been up to testify a couple of times on this issue.

Senator CARPER. Who is that person?

Ms. MANFRA. I am sorry. Angie Bailey. We have a great relationship with her. She has only been on board for maybe 2 years or so. But I am very excited about the program. While it has taken longer than we would have liked, they are completely rethinking the way we think about civilian service and really applying best-in-class concepts of how technology companies hire workforce. The way they are implementing the authority is going to allow us to have a very different approach to our workforce.

We are also trying to improve the stuff we can control, think differently. Does everybody need the highest level of security clearance? The answer is no, because that is often the thing that can take the longest in the hiring process. Are we being better recruiters? We cannot just rely on a website and people to apply via a website. We have to be out there targeting our employees.

As Greg mentioned as well, we have to understand what workforce we want and make sure that we are targeting the skill sets for the workforce that we want and that we need instead of hiring basically the people that are often given to us through the old government approach to hiring. So we are trying to do as much as we can.

Senator CARPER. Thank you. My time has expired.

Mr. Chairman, two things. One, thank you so much for scheduling this hearing and to all of you for coming and testifying. My colleagues may recall that this Committee also required NPPD to improve EINSTEIN, provide us with updates on improvements and features. It is my understanding that we have not received any updates. I might be mistaken, but that is what I am told. I would like for us to have a conversation after today is over, and I will be interested and will ask questions for the record with respect to EINSTEIN 3A. Has it been updated? Does NPPD intend to develop new functions? Those are the kind of questions we would like to pursue.

Again, thank you. This is timely and maybe overdue, but I am just delighted that we are doing it. Thank you.

Chairman JOHNSON. Senator Jones.

## OPENING STATEMENT OF SENATOR JONES

Senator JONES. Thank you, Mr. Chairman. I apologize for being late. We were marking up the opioid bill, which is also a very important piece of legislation that is about to move.

I know you have had a lot of testimony and questions and answers, so I am going to kind of limit this to one question that I would like each of you to address, and it is just a pretty general question.

There have been some 50 bills governing cybersecurity that have passed over the last few years, which sounds like an awful lot of action on behalf of the Congress. I have seen some parts of your GAO report suggesting areas of improvement in the implementation of some of those bills. But I would just like each of you to address, as you can, what else is there? Do you have, for instance, all the tools that are necessary, whether or not you have the ability to implement them right now, are there other things, 50 bills sounds like a lot, but there is a lot going on in this world, and are there other things that Congress and this Committee should be looking at that would help you in this world, whether it is the Department of Defense, whether it is Homeland Security? If each of you take just a moment with that, I would appreciate it.

Ms. MANFRA. I can start.

Senator JONES. OK, sure.

Ms. MANFRA. I would say that Congress has, like you said, done a lot of very effective legislation in cybersecurity and really positioned DHS as that agency that is central to managing the defense of Federal networks and civilian networks and critical infrastructure. We are very satisfied with the authority that we have been given. For us, it is really about how do we ensure we have the capacity and the capability to fully implement those authorities.

But as we continue to work and expand the work that we are doing and learn more about different areas, if we come up with additional legislative remedies that are needed, we would absolutely come and work with this Committee.

Senator JONES. All right. Thank you.

Mr. WILSHUSEN. I think it is more a matter of execution rather than additional legislation for the time being. As you mentioned, there are a number of laws for which agencies are responsible in implementing relative to cybersecurity. But the key thing is taking those authorities and actually effectively and efficiently executing them in order to secure the systems that the Federal Government operates. I would say it is more a matter of execution rather than the need for additional legislation at this time.

Senator JONES. All right. Thank you.

Mr. ROSENBACH. Sir, it is always easier when you are on the outside, but I think that you all could start by clarifying the committee oversight structure for the Department of Homeland Security. This would not be passing a bill back on the Executive Branch, but it would be dealing maybe in the co-equal branch of Congress and cleaning things up here. I was speaking with Secretary Manfra beforehand, and she said she has already testified I think 15 times this year. Having been an Assistant Secretary of Defense, you spend a crazy amount of time preparing to come and work with you all, which is really implement, but it is time taken away from doing operational real things. I know that is a hard thing, but it is worth mentioning.

I think that capability and talent are the two most important things in government, and bureaucracy is deadly to capability and talent, even in the Department of Defense where we have a huge budget and a lot of really motivated people. DHS has that as well. In some ways maybe there is a bill that could do away with a lot of the reporting requirements that GAO then grades Secretary Manfra on. That probably also would be helpful.

I love government. I am at the School of Government. I am a big fan of that. But sometimes too much government keeps you from getting the real stuff done.

Senator JONES. All right. Thank you all, and I appreciate it. I can tell you a couple of things from the report. As a former U.S. Attorney back before this really became such an issue, just the reporting and being able to share information across agency lines, and the collection of that data is so important. In Alabama, in particular, we have such critical infrastructure sectors with ship building and manufacturing, the aerospace industry, manufacturing, so I want to take you up on looking at that, because I think we need to be efficient and I want to make sure we can collect the data and be able to move as quickly as they can.

That is all I have, Mr. Chairman. Thank you so much for letting me sneak in at the last minute and throw a couple questions out.

Chairman JOHNSON. Not a problem. First of all, it was a great question. It was the first one on my list. Do we have enough laws? Mr. Rosenbach, we are going to clip that testimony. You are singing right out of our hymnal. I am sure Senator Heitkamp will make the same point. Senator Heitkamp.

## OPENING STATEMENT OF SENATOR HEITKAMP

Senator HEITKAMP. Thank you, Mr. Chairman.

This is probably the most serious issue that we are confronting, probably behind the pandemic, in this country with the most disruptive oversight process in government. Think about that. When something really bad happens, I can only imagine the scramble to assume who is responsible for not making sure that we have the resources and making sure that we were not on the ball. We have to fix this, and I think the Chairman has held a meeting. It is really hard to wrestle jurisdiction away from other committees, but we have to stand firm to centralize our discussion of this, because if we do not, we are going to miss opportunities.

One of the things that I have been talking about has been the impact of all this on small business, and I want to just make another brief statement. I think sometimes cybersecurity gets overlaid or kind of misstated as a privacy issue. It can become a privacy issue, but it is different from and different than privacy. We need to make sure that when we are talking about this, we do not confuse the two concepts.

The first thing I am going to say is the first line of defense, if you are a beat walker, doing community policing, is people lock their door. They lock their car. They carry a flashlight. They carry some kind of method of defending themselves. They practice some kind of self-defense.

We are missing a national dialogue on what we need to do for self-defense. What can we do within the government to set out some principles? I think the public wants to know. They do not want to have 20-character passwords, because everything requires a password now. They want to have easy access to their data and their information. But they need to understand that they have within their power the chance that could be a back door to something really bad happening.

What are we doing to help cyber hygiene, to really promote cyber hygiene, to get it out not just to small businesses and big businesses, but to get it out to the mom-and-pop users of this technology? We will start with you.

Ms. MANFRA. Thank you, ma'am. Very well said. A lot of talk in cybersecurity and technology is very fancy and all sorts of interesting technologies, but when it comes down to it, my team of assessors continue to find the same basic problems, poor patch management, misconfigured systems, things that are known bad things. Within the Federal Government, we have tried to focus on changing those behaviors.

More publicly, which I think is what your question is really getting at ma'am, we do need to do more. Our organization has been working with an organization called the "National Cybersecurity Alliance" for some time—the campaign has been called the "Stop, Think, Connect Campaign"—for some years, and we have been talking a lot about how do we expand our reach? How do we make the message more——

Senator HEITKAMP. Can I make a recommendation? I just visited with my insurance agents. Great people. They are now selling a product that includes cyber insurance. I am not sure how it is going to work. But there is a great place—when we talk about fire protection—I used to run the Fire Marshal's Office in North Dakota. We partnered with the insurance agencies because they knew they had risk, and they could do a lot.

What are we doing to plus-up our effort looking at private organizations that have some skin in this game?

Ms. MANFRA. Another great point. We have been working with the insurance community for a few years now, both to educate them as they think about developing insurance policies and the challenges they have around that, but as a stakeholder, as a risk manager in helping to raise the level of cyber hygiene through requirements in their policies.

We have been working with them. I think that environment has changed significantly. We are seeing a lot more insurers in this space. We see them as a great partner. Like you said, just getting to the average consumer, getting to—how can people be safe online? How can people be secure online? But also working with the technology community to think differently about things like identity.

Senator HEITKAMP. I do not have a whole lot of time left, but it seems to me that as you experience or see—just like we would do a GAO report with a list of recommendations, if you said, look, Corporation X, you are putting your users at risk, only you know that, and they continue to—if they do not modify or change or make the investment that they need to protect their data, should we not know that as consumers? Should we not know that? Should we not know what you know so that we can then create that push to encourage more rapid change within those organizations that are not doing what you think is appropriate to protect data?

Ms. MANFRA. In the case where I would know that information, which is not usually the case, but in the case where I would, I do believe that, yes, consumers should have a right to know. But that is definitely something that working with the U.S. Securities and Exchange Commission (SEC), working with others, thinking about disclosure requirements, transparency around——

Senator HEITKAMP. The concern that I have is frequently when we talk about disclosure, it is after the breach. It is, OK, now, who are you going to tell, when are you going to tell, and Equifax is an excellent example of where that got totally messed up, in my opinion, people who knew, who were trading before the public knew. That is some of the richest data you can possibly imagine, and we do not know—that is like a ticking time bomb waiting somewhere offshore, in my opinion, until they can absolutely do havoc, so we cannot say, well, nothing happened so far, because, why rush it?

What I am saying is that there has to be a level of accountability with standards that when we look back on it, we could say, look, you should have known. A great example of that is when I met with my folks in Grand Forks, North Dakota. We are trying to really build out some cyber capability. They said a lot of the ATMs were running on Windows 98. Yes, look at your face. I mean, can you imagine? These are the kinds of things—yes, I know it is expensive, but Windows 98 is no longer being modified for security protections. That is the kind of thing the public would be absolutely furious about if they knew that we knew that and somehow now their identity is being stolen, including, Social Security numbers and bank account numbers and now they are in the hassle of that.

I just think it is really important we talk about cyber hygiene, that we talk about creating greater incentives for the easy things to get done—not the tough things, not autoimmune systems, all the things we want to talk about up here, but all the things we need to do here to lock the door, right? That is the example I always give. Let us lock the door. Maybe they will still break a window, but it is going to be harder to get in.

Ms. MANFRA. I could not agree with you more, ma'am.

Chairman JOHNSON. Although it is kind of hard to hack into a floppy disk. [Laughter.]

I do want to reinforce your point on the insurance. I have been making that point for quite some time. That is a private sector model, just like in manufacturing, because you have to respond to insurance premiums. Your premiums are lower if you have your sprinkler heads closer together. I think the insurance industry off of NIST, something like an ISO type of certification process, will be much more flexible than government ever will, as we are talking about needing congressional action just to change the name of your agency. I think that private insurance model is probably one of the best ways of enforcing those standards.

Senator HEITKAMP. It is definitely a force multiplier, and more and more small businesses are coming wanting protection, understanding the risk and the liability. This is an absolute pivotal point. If I can just for a minute brag about my insurance agents, they literally go through a checklist on cybersecurity.

Chairman JOHNSON. Very thorough.

Senator HEITKAMP. What are you doing? What are you doing here? Maybe you should think about that. That is just invaluable. That is the kind of army you need to prevent people sneaking in through the back door.

Chairman JOHNSON. That is because they want the premium. They never want to have to pay out the claim, which is exactly what you want with insurance.

Senator HEITKAMP. That is why you put sprinkler heads close together, too.

Chairman JOHNSON. Right. Senator Daines.

## OPENING STATEMENT OF SENATOR DAINES

Senator DAINES. Thank you, Chairman Johnson, Ranking Member McCaskill, for holding this important hearing. Cybersecurity issues have been at the forefront of many minds lately. I spent 12 years in the cloud computing business, and you always, when you woke up in the morning, ask yourself, "What could happen in our business to put you on the front page of the Wall Street Journal?" It is a cyber breach that is exactly one of those.

In light of attacks such as the hacking of Montana's schools recently up in Flathead County, up near Glacier Park, as well as broader government breaches like the one we saw at OPM, in fact, 28 years in the private sector I never got a letter from my human resources (HR) department saying my PII had been compromised until I became an employee of the Federal Government as a U.S. Senator when I finally got a letter. It is vitally important that we address these issues promptly.

In the Energy and Natural Resources Committee, we have been tackling the issue of protecting our electric grid from cyber attacks. It is a delicate balance we must strike as the vast majority of our infrastructure is privately owned, but many companies do not have the capital, sometimes the expertise, to defend against attacks from bad actors or nation-states. That is why it is important we work with the private sector to bolster cybersecurity.

To that end, I have introduced the Cyber Safety Act, which simply clarifies that cyber technologies can apply for Safety Act protections. This bill would help incentivized the next generation of cyber defenses for critical infrastructure and help protect the grid from cyber attacks.

Mr. Rosenbach, you mentioned in your testimony that, "Bolstering private sector cyber defenses without regulation should be a priority." I agree with that. How important is it to enable the private sector to innovate and commercialize the next generation of cybersecurity technologies without a technology mandate?

Mr. ROSENBACH. Senator, I think it is really important, and during the time I was in the Department of Defense, in the beginning I think NSA CYBERCOM had better capabilities than the private sector. If I look now, 8 years later, it is not even close. The private sector moves more quickly, advances more quickly. We need to be able to rely on them in a way that helps the country in a broader national security sense as well.

Senator DAINES. That is a strong statement you made, and as somebody who has been on the Commerce Committee, I see that as well in terms of the innovation cycles, the innovation ecosystems built in the private sector, and oftentimes how this large bureaucracy that we have, smart people, well-meaning people, sometimes having difficulty to attract and retain the best people when the money is a lot better sometimes on the other side.

Mr. Wilshusen, I believe it is hard for the government to mandate cyber practices on the private sector when it does not even have its own house in order. There have been multiple cyber breaches in the Federal Government that are very concerning. Last year, I helped push the Modernizing Government Technology Act, and just last month, this Committee passed a bill that I introduced called the "Support for Rapid Innovation Act" as part of the DHS reauthorization. Both are important steps to mitigating risks within the Federal Government.

What else do we need to do to ensure that the Federal Government is secure against cyber attacks?

Mr. WILSHUSEN. I do not know if one will ever be able to say that we are secure against cyber attacks, but we can certainly do more to try to reduce the risk and likelihood of having significant breaches at Federal agencies. Much of that, as we discussed, is to effectively implement the security controls and requirements that have already been established. As Secretary Manfra mentioned, many of the key findings that we identify during our audits are the same things that we have been identifying for years: unpatched systems, use of unsupported systems, and not having effective security testing and evaluation processes at agencies.

We often find that agencies will go and conduct a test or review their systems merely by either conducting interviews or reviewing certain policy documents as opposed to actually examining the security and the configuration of its systems.

Much of what we need to do in the Federal Government is assuring that agencies have sufficient information on what the key cyber threats are at the moment, establishing processes to assure that they securely configure their systems, and being able to assure that those configurations and controls are being reviewed on a regular and ongoing basis.

One of the programs that DHS is spearheading, the Continuous Diagnostics and Mitigation Program, is intended to help along those lines. But it is still in the relatively early stages of implementation. It is going to Phase 3 this year. There is still much that needs to be done at the Federal agency level.

Senator DAINES. Thank you. One of my observations, too, in terms of the procurement of best practices, best technologies out there, we see some of the same challenges in the Federal Government that are reflected oftentimes in Fortune 100s where Chief Information Officers (CIOs) and Chief Technology Officers (CTOs)—there is the old saying, "You never get fired for buying"—and I will not create any problems here, but you can kind of list some of the large enterprise companies that typically they have Italian suits, expensive shoes, and high billing rates, and technologies that sometimes are burdensome and it costs more money to upgrade them and implement them than the solution itself. I will just leave it at that before I get in trouble.

But my point is to be looking for these smaller, nimble players out there that are oftentimes on the forefront of innovation. I speak as one who used to be there. We finally got acquired by a large corporation, but some of the best ideas, frankly, are out there with little guys at the moment, and I hope we can incentivize appropriate procurement that would allow us to look at some of these smaller, more nimble players that usually are less money, better solution, faster implementation.

Mr. WILSHUSEN. You mentioned procurement, and that is another key area to helping secure Federal systems. One aspect of that is buying operating systems, that the vendor has already preconfigured securely. By acquiring software that is secure out of the box, it will also help with securing systems.

Senator DAINES. Some of these large technology dinosaurs are extinct. They just do not know it yet. They need to be looking at the next generation.

I better be quiet here, Mr. Chairman, before I get in trouble.

Chairman JOHNSON. You were close. Senator Hoeven.

## OPENING STATEMENT OF SENATOR HOEVEN

Senator HOEVEN. Thank you, Mr. Chairman.

Ms. Manfra, Senator Peters and I have introduced legislation, the Federal Cyber Joint Duty Program Act, S. 2620, which would enable the Federal Government to establish a civilian personnel rotation program for employees with cyber designation. It is similar to the joint duty programs that exist in the military and the intelligence community.

My first question is: In your experience have you noticed a governmentwide cyber workforce shortage and/or retention challenge in the cyber field? What are the impacts that that has on your office, agency, and government as a whole?

Ms. MANFRA. Yes, sir, we absolutely have a shortage. We also have an equal challenge of inconsistently trained and qualified professionals across the government. We are working to address both of those challenges.

Senator HOEVEN. Do you think a rotational program for civilian employees in cyber work roles such as the bill that Senator Peters and I have introduced can be used as a tool to further develop and retain talent and create some of that consistency in the cybersecurity career field?

Ms. MANFRA. Sir, we would look forward to working with you on the specifics, but, yes, the concept makes a lot of sense to me.

Senator HOEVEN. That is a good answer.

Mr. Wilshusen, I guess you published two reports recently which outline the persistent and longstanding challenge the Federal Government is experiencing in this area. I would ask you the same questions.

Mr. WILSHUSEN. Certainly, as you point out, that has been a longstanding challenge within the Federal Government. Some of our reports and surveys that we have conducted with agency CISOs have consistently identified obtaining and retaining staff with technical skills has been particularly challenging for them. One of the steps, as you mentioned, with the rotation aspects, could potentially help in terms of giving those individuals greater insights as to how different agencies are implementing security for their systems and may be beneficial not only to the individual agencies but to those individuals as well.

Senator HOEVEN. I would ask the two of you, and then Mr. Rosenbach, relative to the private sector, in the public sector, how should we be communicating to the public in terms of cybersecurity, the steps we are taking, and what assurances can we give them that we are addressing cybersecurity sufficiently, first in the public sector, then in the private sector, both in regard to State actors, be that Russia, China, Iran, North Korea, and non-state actors, terrorist groups, for example? How should we be talking about what we are doing and its adequacy and whether or not they can be reassured and where they should have concerns?

Ms. MANFRA. From my perspective, sir, the way that I talk about it is that we are taking a risk-based approach to cybersecurity, and I cannot assure that there will never be another data breach or that we will never have a significant cyber incident. What I can assure is that we are taking a very focused look at what we are calling "national critical functions." What are those functions that our citizens and residents and companies depend upon? How can an adversary disrupt those functions, whether that is through some sort of cyber means or otherwise? How do we work to reduce that risk, whether that is in the Federal Government or within critical infrastructure?

We have a lot of authorities, not just DHS but the government-wide has a lot of capabilities. We have a thriving cybersecurity market. We have increasing awareness among communities and companies of things like the NIST Cyber Framework where we need to continue to raise that baseline level of cybersecurity.

For me, the approach is a combination of improving our understanding of threat, vulnerability, and consequence, but I come at it from the vulnerability and consequence side. What are those really high-impact—where do we have public health or safety risk? What are we doing to reduce that? For me, it is mostly focused on nation-state actors because those are generally the ones that both have the capability and the intent to accomplish something like that. But we are also looking at other non-state actors who would seek to disrupt those services or functions.

Does that answer your question?

Senator HOEVEN. Kind of, but, again, for the public that gets to be a little confusing, and it comes across you are working on it, but in terms of should they be reassured that you have this, that kind of answer, it is hard to say you get them there with it.

Ms. MANFRA. I know that people want assurances. But in security——

Senator HOEVEN. They want honest assurances.

Ms. MANFRA. Sure.

Senator HOEVEN. They want an accurate response.

Ms. MANFRA. What I can assure the public is that the Department is doing everything that we can to coordinate within the government to make sure that the intelligence community is collecting information that would help reduce the risk, that we are passing that information to those who would own it, and that we are gaining visibility into what these potential consequences would look like. Companies are stepping up—the financial sector, the electric sector, water utilities across the country.

Is there a lot more that we should be doing? Absolutely. But people are stepping up to own the risk and to work with us on it.

Senator HOEVEN. Mr. Wilshusen, how would you put it?

Mr. WILSHUSEN. I would probably say that we are never going to be completely safe, and I think as you say, you have to be honest, particularly—and it is not just the Federal Government, but it is also individuals and their behavior out on the Internet. There is a great propensity for people to share a lot of information out on the Internet, on various different applications, and that information is being collected and used, often unbeknownst to the individuals who provide that information, generally willingly, to many of the different applications and systems that they may frequent out on the Internet.

I think in terms of just being able to provide assurance to say that we are doing everything we can is one aspect of it as a Federal Government, but, we also have to be able to demonstrate that we are doing everything we can do to protect the systems that the Federal Government operates.

But it is also up to individuals, who need to recognize they, too, have a responsibility. As the old adage says: security is everybody's business. Individuals, citizens, also have to take ownership of it as well in terms of how they act and behave in cyberspace.

Mr. ROSENBACH. I will be very quick because I know you are over. I will say that the most important thing to me is that you cannot expect the Department of Homeland Security or the private sector to be defending against advance nation-state threats. You need the Department of Defense and the intel community to be operating outside U.S. borders to take on adversaries before they hit us. The idea that we would let someone attack our democracy and our election system and there be almost no price to pay for that still is crazy to me. I was in a job where I probably should have done more. We as an Administration should have done more. But the country needs to do more.

The private sector, there is a great and thriving market in the cybersecurity market, and they can make money and make a big difference. However, there are parts of the tech sector that need to internalize that they have a responsibility to the public to do more. That is primarily social media platforms right now. There is, I think, a little momentum in a positive way, but we need to see more there. Information operations by nation-states will continue to get worse unless they and the government both do something that is a little more assertive.

Senator HOEVEN. Thank you. I appreciate it.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator Hoeven.

I have a number of questions, but Senator McCaskill is on a tight schedule, so I will let her ask hers first, and then I will close out the hearing.

Senator MCCASKILL. Thank you. I just want to echo your comments, Mr. Rosenbach, about our lack of response offensively to the Russian active war against our country. I had the opportunity in the Armed Services Committee to pointedly ask Admiral Rogers, conveying to him what a woman said to me in the grocery store. Can we stop them? Do we have the capability of stopping them? He said to me in that hearing, "Yes, you gave her the right answer. We can." But have we? He had to admit, no, we have not, and that he had not been given the command to do what we need to do to offensively go after this act of war against our democracy. It is a real head-scratcher for me and very frustrating that we are dancing around the obvious here. I just wanted to echo your comments that we are not utilizing the assets of the Department of Defense in an effective way against Russia and what they did to our country.

Director Wilshusen, I wanted to ask you—I know it was the Election Division that gave—this is the last question I have—that did the report looking at the voting equipment and the voluntary voter system guidelines. The Election Assistance Commission has guidelines they use to certify systems, which is pretty important right now. Those guidelines were first released in 2005, very outdated. I think anybody would acknowledge in this area that using guidelines that were developed in 2005 is not appropriate.

They were updated in 2015, and the GAO's report that was issued last month noted that in January 2016, EAC adopted a plan that all new voting systems would be tested and certified against the 2015 guidelines beginning July 6, 2017. They also noted that as of November 2017 no voting systems had been certified using the 2015 guidelines. Looking on their websites, some systems were certified in March, like a month ago, but to the 2005 guidelines.

What is going on? Why are they not utilizing the new guidelines that we have worked hard to update to make sure that the certification has the kind of validity we need at this point?

Mr. WILSHUSEN. I will probably have to get back with you on the answer to that question with the audit team that actually performed the work. But I will say that my understanding is that the Election Assistance Commission is actually still in the process of updating those regulations or those voluntary guidelines, and they expect to issue them later this year. But at the same time, it would seem that if there are more current standards, that they would be using those standards to measure against new systems that are coming online.

Senator MCCASKILL. Can you add anything to this, Secretary Manfra? What is the holdup here? This seems really like a waste of time to be certifying to 2005 guidelines?

Ms. MANFRA. Yes, ma'am, those guidelines are not final yet, so even though they did update and draft them, they are still in the process of finalizing. My understanding is that they will be finalized and issued very soon, and I agree with you, it is too long. I know the EAC has been working very hard, and we should get some updated guidelines out in the next few weeks, is my understanding.

Senator MCCASKILL. I will continue to follow up on this. I will follow up directly with the EAC. But is this some requirement they have to make it take this long? Or are they just not moving quickly enough?

Ms. MANFRA. I would definitely check with the EAC on this. My understanding is it is somewhat of a cumbersome process that they go through. But I would definitely confirm with them.

Senator MCCASKILL. Yes, because they should probably quit certifying until they get the new guidelines out. I think it is going to give a false sense of security to a lot of States.

Chairman JOHNSON. Thank you, Senator McCaskill.

I really do have a pretty long list of questions here. I think the questions asked by my colleagues have been excellent, but this is a big topic.

Let me start by saying, when I got here in 2011, it was just generally recognized that cybersecurity is a real issue and we have to do something about it. There was one proposal made, I do not know, 400 pages. I was asking the folks that would be tasked with implementing it how long would it take to just write the regulations, and I am quite sure that they said something like 7 years. I never really thought a government solution here was going to be the be-all, end-all. You really had to look to the private sector.

But in those hearings—and I thought this was pretty good, and I want to see if this is still a pretty good outline of what we really face in terms of threats. Four points.

Cyber crime, cyber theft, the ransomware, copyright infringement, cyber intrusions all for the purpose of cyber thefts gaining people's personal accounts and personal information so they can hack into your accounts. We have seen them obviously violate the Internal Revenue Service (IRS) files.

Then the next level would be industrial espionage. Of course, we have seen from the Mandiant report China has been excellent about that, and they have a lot of U.S. technology because of that. But it would not necessarily be only isolated to nation-states.

The next one would be national security espionage. It is pretty amazing how close the J–20 Chinese fighter is to our F–22. Amazing.

The final level is really cyber warfare. Now, you could argue that could be destructive warfare. It could be disinformation.

First of all, are there other categories that we need to be worrying about? Is that a pretty good outline to describe what threats we face? Secretary Manfra.

Ms. MANFRA. I can start, and my colleagues can add. First of all, I think, yes, it is a pretty good construct. The first group I might recharacterize as say "monetization," so organizations, they do not have to be criminal, but they are seeking to monetize what they steal. I think you are right around it is differentiating between industrial espionage and national security. We further differentiate between a State—using State assets to conduct industrial espionage for the benefit of their companies.

The last one, cyber warfare, I guess the distinction that I would make is because cyber warfare means a lot of things to a lot of people, but it is the position of holding our critical infrastructure at risk and getting into that geopolitical nature of because I believe we have supremacy in most other areas of security through our Department of Defense, nuclear, etc., we have a lot of countries that are seeking to exploit an asymmetric advantage.

Now, whether that leads to actual warfare or if it just puts us in a position where conflict and escalating tensions means something different because of the risk we have in the homeland, but——

Chairman JOHNSON. Part of the problem is we really have no definition for it, correct? If you destroy computers through electronic beams, we call that a cyber attack. If you destroyed those computers with a bomb, that would for sure be an act of war. Do we need a definition? Could we even come up with one?

Ms. MANFRA. I think we need a doctrine for cyber war, and we are working on that. It is complicated. There area lot of people who have done a lot of work on this. But I do believe that is something that is important, and I think it is important to be transparent about what that doctrine looks like to a certain extent.

Chairman JOHNSON. Mr. Rosenbach.

Mr. ROSENBACH. Sir, this may sound overly simplistic, but for about the past 10 years, I have always heard people debate whether we need cyber doctrine or what cyber war is. In my mind, in all of the White House Situation Room meetings I sat through, people knew——

Chairman JOHNSON. You know it when you see it.

Mr. ROSENBACH [continuing]. What a real attack was. The problem is: Are you going to do something about it? It is not in the definition. You know it. It is are you willing then to take the action to go back and do something about it.

Chairman JOHNSON. I realize there is a spectrum here, but what about just the challenge of attribution? You retaliate, you respond. If you do not have the attribution correct, that is a real problem. We just saw that with the use of chemical weapons.

Mr. ROSENBACH. Yes, sir.

Chairman JOHNSON. When we finally could attribute it and we had a high level of confidence, we responded. But it is more difficult in cyber, isn't it?

Mr. ROSENBACH. Yes, sir. It is difficult. I would say this is something that has really changed over the past several years, too. Attribution is not as difficult as people think. The private sector is very good at it, if you look at Mandiant-CrowdStrike, firms like that. NSA is very good at it, even some of the experts at DHS. You will never have 100 percent confidence. Just like in the terrorism strike, you may not know definitively, but most times now you can have pretty good attribution, and you can have it pretty quickly.

Chairman JOHNSON. Let me ask you what kind of cyber attacks actually keep you awake at night. This is where I am going to get into the prioritization, the things that we really need to be concerned about, which means that is what we need to prioritize our assets and our attention toward as well. I will stay with you, Mr. Rosenbach.

Mr. ROSENBACH. Yes, sir, in your opening statement you talked about maybe the election threat is a little overemphasized, and in some ways that may be right. But what I worry the most about is a combination of info attacks and cyber attacks done by any of those nation-states. The Russians were successful in some ways, but that will not be lost on Kim Jong-un or the Iranians, and they will want to go after our and other democracies. They can do things that undermine trust in democratic systems. They are not just about elections. The financial sector——

Chairman JOHNSON. Don't we play into their hands in terms of undermining by literally blowing it out of proportion? I am not in any way, shape, or form minimizing the seriousness of it. We have seen what they did in Crimea, Ukraine.

Mr. ROSENBACH. Yes, Senator.

Chairman JOHNSON. Basically an act of war against Montenegro if it would have succeeded.

Mr. ROSENBACH. I totally agree, and I did not mean to mischaracterize your statement.

Chairman JOHNSON. No, we are having a discussion here.

Mr. ROSENBACH. I totally agree with you. Other things I worry about that are very important to the way the economy and the country runs, our GPS vulnerable to attack, other systems like that that these advanced bad guys know we depend very heavily on. In the Department of Defense, we always worried that someone would take out some of our network that would prevent us from responding in an operational way. Just an attack on our weapons systems, which are very network-dependent, always kept me up at night.

Chairman JOHNSON. What about attacks on the Financial System?

Mr. ROSENBACH. Yes, sir, right.

Chairman JOHNSON. We have seen them shut down the electrical grid in Ukraine.

Mr. ROSENBACH. Twice, right, for sure.

Chairman JOHNSON. These are existential just about, correct?

Mr. ROSENBACH. Yes, sir. Those are all real things. With the financial sector, they realize that a loss would hurt them. They tend to spend way more money than any other sector, so that is positive. They tend to be very good. There are a lot of things that worry me on the spectrum. But, again, your point about the fact that we are watching all of these things happen, the Russians take down the power grid in Ukraine twice, and then our response—and this was during the time I was in there—was weak to none. That is not a good way to improve our overall security at a national level.

Chairman JOHNSON. Secretary Manfra, in your testimony you talked about, somewhat vaguely—and, again, I do not want to get into classified information here, but we are aware that Russia has done far more than meddle in our election. But you talked about attacks on staging versus intended targets. First of all, can you define that for me? Can you in a public setting lay out as best you can what Russia has done in other critical infrastructure outside of the elections?

Ms. MANFRA. Yes, sir. The difference between a staging or intended would be if somebody was trying to get a database that holds critical data that they want in a company, that company maybe has really good cyber defenses, but they are going to look for other targets that the company may have a business relationship, for example, and they are going to infiltrate that company and then try to jump to their ultimate target. We see that a lot. We see a lot of what we would call 'staging targets' where they are looking particularly for companies, what are the business relationships, what are their supply chain vulnerabilities. Even though a company itself may be doing everything it can, they are vulnerable because they have those other connections.

We have talked publicly a lot about what Russia is doing. We have issued an unprecedented number of alerts attributing to Russian activity. We issued the alert around the targeting of critical infrastructure. It was not that they got into the control systems. We were able to disrupt that before they—if that was even their intent, but before they got there. But we are concerned about what they were stealing, the schematics of the control system, for example. We wanted to ensure that everybody had access to this information and could defend themselves.

We have also issued this alert around network infrastructure devices, around routers, and these are really core to how networks and the Internet actually run. If an adversary can have access to that router, for example, they essentially can do pretty much whatever they want with that traffic.

Chairman JOHNSON. Let me quickly interject. How did we let Kaspersky Labs grow the way we did, knowing what was the potential there, let them become one of the largest security systems in devices throughout America? Why did the intelligence community, why did we allow that to happen? Why did we not blow the whistle on Kaspersky years ago? Can anybody answer that one?

Ms. MANFRA. I believe in a free and open market where those who have the best product can sell that product. That being said, the FBI and others and ourselves have been providing classified briefs to various different organizations in industry.

What I felt was that we needed to do more. We needed to get the word out.

Chairman JOHNSON. Were we unaware of the fact that the owner, the head of the company, was KGB-trained? Were we unaware of that for years? Did that just kind of slip by unnoticed?

Mr. ROSENBACH. No, sir. That is something that has been widely known. Having very granular intel on things like that is hard. In the Department of Defense, we were always much more skeptical about Kaspersky, and so I think very rarely used it.

The point about Kaspersky that is worth maybe internalizing is probably the best marketing person for Kaspersky was Edward Snowden because all around the world people then doubted whether you could trust American cybersecurity firms, and a large part of the world decided they would trust Kaspersky more.

Chairman JOHNSON. Russia.

Mr. ROSENBACH. Right. That is a very unfortunate thing, but at least the rest of the world now is under surveillance by Kaspersky but not as much of the United States.

Chairman JOHNSON. OK. I interrupted your response to my question, though. Did you have anything else you wanted to say?

Ms. MANFRA. On Kaspersky, sir?

Chairman JOHNSON. Yes.

Ms. MANFRA. No.

Chairman JOHNSON. I appreciated Senator Jones' questions in terms of number of laws, and I had the exact same question, so let me pose it somewhat differently. I think the response from both of you is that we do have the authorities, we have the laws. I will ask: Do we have too many? Are there overlapping laws? Are there conflicts in those laws that create problems for you? Or just the sheer volume—again, some of these, we are not complying. It does not sound like we are complying at all. On the 0 to 10 scale, it is probably 0. Is that because we have just passed too many that it has taken the Department's eye off the ball?

Mr. WILSHUSEN. I do not know if we have too many. Specifically, there is some overlap in terms of what agencies are required to do, either per law or by government policy. Often, some of the laws that are passed codify practices that agencies and DHS are already doing. While there is usefulness in that, it helps to memorialize and make that a continuing requirement, such as with NCCIC, for example. There is usefulness in codifying practices so they endure past different administrations. But I do not know if I would say that there are too many laws related to cybersecurity.

I will go back to what I said earlier, that it really gets back to execution, and there is not sufficient execution of those laws that are there or the implementing regulations and guidelines that have been identified by either OMB, DHS, or NIST.

Chairman JOHNSON. Any of you want to comment on that question?

Mr. ROSENBACH. Sir, I know when you are in government, it is often hard to say something officially on the record about there being too many laws, so this is what I would say: When I was Chief of Staff at the Department of Defense, the last year the National Defense Authorization Act had 1,500 pages of new laws. The year before that, it had 1,400 pages of new laws. If you go through and you put all those together, it really binds the hands of executives in government no matter what the department.

In the case of DHS, when they have all these overlapping jurisdictions, it makes it even more complicated because then they will be testifying on maybe the same law or theme for several different committees.

I think there is something here that is not right about the way government is working. My humble perspective.

Chairman JOHNSON. I do not know too many organizations that would recommend having a 535-member board of directors.

Mr. ROSENBACH. No, sir.

Chairman JOHNSON. We have kind of seen the results.

Secretary Manfra, do you have a comment?

Ms. MANFRA. We have not done the analysis to answer your question specifically, though we would be happy to work with you on that. I think from my perspective I feel that we have the laws that we need to execute our job, and as Greg said, it is a lot about capacity to actually execute. I think what we are doing is looking across, whether it is laws, reporting requirements, or regulations, where there are unnecessary burdens that are either put on the private sector or Federal agencies or whether maybe it is something useful but needs to be implemented better. I know that is a fairly broad answer. It is only just because I do not have specific analysis.

Chairman JOHNSON. I will tell you, my attitude toward this, being Chairman of the Committee with jurisdiction over DHS, is we will get referred to us all kinds of different bills that have either passed the House or that are proposed by Senators, and we take all those very seriously. But we also take our responsibility to make sure that the Department is in—and I do not want to say "total agreement" because sometimes you have to potentially, with oversight do corrective action. But you sure would like to be cooperatively working with the Department to make sure that what is being passed out of here is complementary and helps you succeed in your mission, which is one of the reasons that our DHS authorization—and Senator Heitkamp was helpful on this as well, recognizing just this oversight and the number of committees of jurisdiction here, every time I ask I get a different number. It keeps getting higher.

In that DHS authorization, which is why I am really hoping that we get that on the floor and pass it in its entirety, would be at least a commission, because there are not many committees or subcommittees that are just willingly going to give up their jurisdiction. But they need to understand—and, that is why, Mr. Rosenbach, I really do appreciate your testimony there. It is madness, and from my standpoint I think it puts at risk our national security and our homeland security. I think that is just true.

Secretary Manfra, you talked about having the authorities, and I know in our briefing on election security, it is the point you made as well. Now, maybe you have changed because you seem certainly open or appreciative, and I think we all appreciate the efforts here. Do you still believe when it comes to your role making sure that we have free and fair elections and they cannot be tampered with, does the Department have enough legal authority to do what you think needs to be done?

Ms. MANFRA. Recognizing that this is a voluntary partnership, and I believe that is the right partnership model, I do believe that we have the authorities and the legal mandates to accomplish that mission. As we mentioned, we appreciate the $26 million. We have a fairly broad mission. We have a lot of critical infrastructure, to include election security, to include defending 101 Federal agency networks. I keep going back to authorities, very important, and we are grateful that we have them. But we also need to ensure that we have the capacity to execute them.

Chairman JOHNSON. One aspect of security is just creating modules that are completely separate. I do want to step through a set of questions. Again, let me emphasize, I believe this is a very serious issue. As Chairman of the European Subcommittee on Foreign Relations, I have seen Russian interference for years. We have held hearings on it, OK? The political assassinations, what they have done. I do not underestimate this. But at the same time, I do not want to be playing into Putin's hands in terms of creating this great doubt in our election system. I do want to hopefully provide some reassurance.

Let me start off, we spend billions of dollars—I am not a real fan of the professional political campaign class for a number of reasons. A lot of that money is wasted. What did Russia apparently spend on Facebook? Was it even $1 million? How effective is any political advertising? That would be my first point.

But in terms of voting machines, lest anybody think that they can be manipulated through the Internet, Secretary Manfra, are any of them connected to WiFi or to the Internet?

Ms. MANFRA. The best practice is to not connect them, and all the State and local officials that we talk to, they assure us that they do not.

Chairman JOHNSON. They do not. Now, some of them have no capability—correct?—although some do have WiFi, they are WiFi-capable, and maybe that is something we should do, is make sure that those are disabled.

Ms. MANFRA. That is correct. Not all of them have that WiFi, and they should absolutely be disabled.

Chairman JOHNSON. Now, the concern in terms of Russian meddling, to me it would be three-fold. First of all, could they get in and get into the voting machines and actually affect the tallies? Next is: Can they get in the voter file? By the way, I am concerned about voter files that are not updated by election officials on the State and local level. That is a concern. Then I think finally it really is the sowing of confusion, the disinformation, doing exactly what the Obama Administration was trying to prevent in its briefing in September 2016, is get the American public questioning the legitimacy of an election.

Let us go through affecting the vote tallies. How probable is that?

Ms. MANFRA. Our assessment is that it would be nearly impossible to achieve that undetected.

Chairman JOHNSON. Anybody want to dispute that?

Mr. ROSENBACH. I do not know. I do not know anything from intelligence. What I do know is how good the Russian intelligence services are, and all the things they did to the Department of Defense even in classified networks. I personally find it hard to believe that we would always be able to detect whether the Russian intelligence services were penetrating into that.

Here is a scenario. Sir, you know how dependent a lot of the States are on vendors. There is no way those vendors' networks are so secure that the Russians hypothetically could not get in supply chains. There is not a great risk. That I completely agree with. But there will always be some.

Chairman JOHNSON. Which is one of the reasons in my voting, we do it on a paper ballot, and we put it in an optical scanner, and you have the paper trail right there.

Mr. ROSENBACH. Yes, sir. That is right.

Chairman JOHNSON. One of my favorite sayings is, "All change is not progress. All movement is not forward." As we have upgraded to more electronic voting machines, I am glad that in my voting precinct we do not do that.

Mr. ROSENBACH. If I could say something, I do not want to interrupt the flow of your questions, but the folks from Wisconsin and the election team there came to the Kennedy School and literally have been probably near perfect partners in terms of all of the States who we have worked for. We had a team that went to Wisconsin, looked at what they were doing, and learned from them. They came and helped us design a tabletop exercise for the other States. They participated in our tabletop exercise. It is those people who are very good about thinking about resilience, and they get the problem. That is what gives me the most confidence, because they are there, they are working on it. It is not in the abstract that their systems——

Chairman JOHNSON. The reason I am taking the time and going through these details, I want to restore some confidence, because I think a lot of confidence, because I believe we need to take it seriously, but let us not blow it out of proportion. Let us in public display, talk about what the true risks are. In terms of actually changing the voting tallies, very difficult to do electronically—not impossible because they share vendors, but those machines are offline. What are the controls in place? You have election observers, Republican and Democrat, maybe Independent, at most voter precincts. Now, depending on how Republican or Democratic a precinct is, the effectiveness of that might be an issue. But we have exit polls, we have pre-polls. Describe the controls that are in place at a local electionsite to hopefully give the public confidence that the vote tallies are going to be very difficult to change enough for them to have an effect, to really affect the outcome of an election.

Ms. MANFRA. Yes, sir, and I think you phrased it perfectly actually in the beginning of the hearing, it is about mitigation, and it is about risk mitigation. What we learned—and we spent a lot of time with election experts in 2016, because, again, we try to take a risk-based approach. We cannot fix everything. We cannot perfectly secure everything. We cannot defend everything. But what we can do is learn enough about the risk and help people prioritize. A lot of cyber people like to think about cyber solutions to their problems, but the reality is that we have a very decentralized, for better or worse, election system. We have a lot of observers in the process, and we have a way of tallying votes from that local polling station all the way up to the State that led us to that conclusion that there were so many observers in the process that somebody would note, there would be an indicator if something was wrong. That was where we got to this judgment.

Yes, there are security researchers and hackers out there that can get into a voting machine, absolutely. But that is not the way it works on an actual election day. These machines are protected in warehouses, physically locked up. They are then transported in a physically secure way to these polling stations.

Now, again, is this 100 percent trying to remove all risk? We are not.

Chairman JOHNSON. No, listen, there is voter fraud. How extensive in my own mind probably not all that extensive except in a very close election maybe to affect the outcome.

Mr. Rosenbach, either agree or disagree or dispute it? What are your thoughts on that?

Mr. ROSENBACH. No, sir, I agree, and, our project is just one small thing. It is not the Department of Homeland Security. But we have been trying to do the same thing. We have these playbooks where State and local election officials see all these best practices. They have been super-receptive to that. They understand that this is a system of systems. It is actually least often the case that we worry about the election, the electronic voting machine itself, as opposed to everything else that could be in there, and the way that you respond to that, just as you mentioned, is really important, incident response. Even if there were hypothetically something, if the Secretary of State with the local election officials came out and explained what may have happened, how you mitigated for that, then the public is much more likely to say, "OK, this looks like something I can trust. The bad guys tried to get in. Maybe they did a little bit. Here is all the evidence."

We have found that that public communications aspect is more challenging than any of the technical part, because probably for very good reason, most State election officials are not really eager to get out in front of a camera and talk to the press about something that is as complex as a possible cyber info attack.

Chairman JOHNSON. But, again, that is what we are trying to do right now, is reestablish some confidence that there are audit trails, there are recounts, there are things that would show up that you would really start scratching your head and go, “There is a problem here.” Let us say the vote totals exceed the number of people registered in a particular precinct, we should actually have some examples of that as well. But, that maybe is not malicious outside actors. That could be just an example of voter fraud.

Ms. MANFRA. Yes, sir, and if I could just add one thing, since you mentioned auditing, we do encourage all States to have an auditable trail. Not all of them have it. I was referring to kind of the checks and the balance and the observation of the vote count. Having an ability to go back forensically review and audit what happened I think is important. I want people to understand that there are some States that still do not have it.

Chairman JOHNSON. Let us talk about the next area that there could be some mischief in terms of voter files. That could be malicious actors outside through—this I think would be more concerning, which is one of the reasons I was not willing to leave that briefing and September and say I have complete confidence, because I learned in that briefing that Russia had attempted to access voter files. That could be a problem. But, how would that manifest? How would that show up? You potentially go to your polling place and your name is not on it, or a bunch of people’s names are on there that should not be on there. Also something that could come to light in the election, but that is exactly what, for example, a country like Russia would be trying to do, is try and disrupt the election, delegitimize it, produce a lack of confidence, correct?

Mr. ROSENBACH. Yes, sir, that is right. In our research we found that, again, election officials are used to doing business continuity planning. They are used to being resilient, because something bad always happens in an election—the weather, electricity. The backup of the voter files in most cases was something they were doing on a regular basis anyway. Even if, depending on the State, on election day a certain name was not on there, they have established standard operating procedures (SOPs) for how to deal with those things. That is another risk-limiting type function in the overall risk mitigation strategy that you would use.

Chairman JOHNSON. They can do, what do they call it? Not a probationary ballot, but a——

Ms. MANFRA. Provisional ballot.

Chairman JOHNSON. Provisional ballot, right.

Anybody else was to comment just in terms of the voter files? If you have a backup and then somebody hacks into it, you are comparing those two, you can do a blend and go, “Oh, there is a problem here,” right?

Ms. MANFRA. Our assessment of the risk related to voter registration files and why we are concerned about it, not just because we had instances of it happening and being targeted, again, it is not so much about the privacy of the information because many of those registration files are not necessarily private. What it was about is to your third point, an ability to potentially sow confusion on voting day. Even though a provisional ballot is available, if you are concerned, was and remains, if people think that they are in the wrong place, they may decide, OK, well, I do not have time, or the lines get long, it is those sort of more—I guess it would generally fall in the information operations side. But that sort of is why we were concerned about voter registration databases.

Chairman JOHNSON. OK. My point in spending a fair amount of time on this is to lay out the facts, lay out the reality, and provide some level of comfort that there are a lot of checks and balances in this process. I think the decentralized nature of our elections provides even greater security. Is this a serious issue? Sure, and we need to take it seriously, and we need to strengthen those controls. But I do not think we should blow this out of proportion and call into question the legitimacy of either past or future elections. That is kind of my main point. If you want to make a final comment on that before I move to my next points, Mr. Rosenbach?

Mr. ROSENBACH. Sir, the only thing I would say is I completely agree that this is not about the previous election. It did not impact the outcome. The point for me is the idea that any other nation could or is designing to impact the outcome of our elections and influence our democracy is something that I think upsets every American and is exactly what you are saying——

Chairman JOHNSON. I agree. But, my point is what keeps me awake at night is shutting down the electrical grid, hacking into our financial system. You want to talk about chaos, that would be it right there. Yes, take this seriously looking forward, strengthen our controls, but there are an awful lot of controls in place that give me a fair amount of confidence, which puts this in terms of my things I worry about lower on the priority list. We have to be cautious not to blow it out of proportion.

Let us just use an example. The fact that we were not able to attach to the omnibus the renaming of NPPD, somebody had an objection. What type of turf wars are existing within this realm? We have DHS, we have DOD, we have NSA, and we have the intelligence community. Do we have stovepipes? That is one of the lessons we learned from 9/11. We had stovepipes; those needed to be broken down. We need to work cooperatively.

Mr. Rosenbach, you were talking about kind of a national center for this, which from my standpoint, when you have to have the private sector liaison plugging into some form of government, you want a civilian agency like DHS. Yet we have resistance to that. Let us lay out the reality of what we are dealing with here.

Mr. ROSENBACH. I really have no idea why someone would object to NPPD changing their name. That seems to me one of these extremely crazy cases of government where an organization cannot even rename themselves. We should probably do a case study at the Kennedy School about how inane this can be sometimes.

Chairman JOHNSON. It requires an act of Congress. It is bizarre to me.

Mr. ROSENBACH. Yes, sir. It is not you, but people can pass all these laws about DHS, and they cannot even name themselves? Humble outsider, but it seems crazy.

Chairman JOHNSON. We will clip that testimony, too. [Laughter.]

Mr. ROSENBACH. It is interesting. If I think back to when I was first Deputy Assistant Secretary, which was almost 8 or 9 years ago now, we did not get along with DHS, and no offense to Jeanette, but DHS was kind of a mess. There were a lot people saying put DOD in charge of domestic cybersecurity, which would have been a horrible idea. We worked it out. There was one very memorable time when we were here in the Senate, and we did a tabletop exercise for the entire full Senate. Senator Mikulski, after the tabletop exercise, pointed to the Cabinet, and the Obama Administration said, "Who is in charge when there is a huge cyber catastrophe?" No one there could actually understand, and so we worked through that. Things are much better now. We are making a lot of progress.

Chairman JOHNSON. Could they answer that question now?

Mr. ROSENBACH. It is very clear. It is actually DHS. In terms of incident response, they know that they are in charge. Now, in terms of the hit back, that was DOD. But even those things were not clear at the time, so there has been a lot of progress, which I think is good.

That said, it now comes to the capability point. When I talk about an idea I have about DHS having more capability to do domestic cybersecurity things that could help critical infrastructure, that is what gives them cachet with the private sector and with others, is if they bring something to the table.

Chairman JOHNSON. Secretary Manfra.

Ms. MANFRA. I do not think we were a mess. [Laughter.]

Chairman JOHNSON. You can always improve.

Ms. MANFRA. It is good to testify next to former government officials.

I think that Eric raises a really important point, though, that the government as a whole has matured a lot in thinking about cybersecurity and just generally how cyber is something that is a part of nearly every mission that we do, whether you are a trade agency, FEMA, or the Department of Defense, the notion that we operate on these systems and they are critical to our mission; but also that we have a lot of capability in the government to deter and to disrupt the threat.

My Department has, I think, matured a lot, as we have talked about quite a bit. We have had a great deal of authorities in the past few years that we did not have previously. That I think helps. We have had significant growth in my organization. When I first started there, 11 years ago-ish, we had maybe 100 or 150 people, and now we are authorized up to 1,000. But we have a really big mission.

I have never received anything but full support from, whether it is the intelligence community, CYBERCOM, or DOD. What I do think is that we have to continue to ensure that everybody is positioned to think about how do we best defend our networks. How do we use the information and the tools that the government has available to it that is unique and ensure that we defend that? I believe it is DHS' role to drive that conversation, and I think as we have matured and we have learned from industry, we are better at doing that within the interagency.

Chairman JOHNSON. You have been at NPPD how long?

Ms. MANFRA. Ten and a half years.

Chairman JOHNSON. OK, so you have spanned administrations, which is good. That provides a little bit of comfort.

Mr. Wilshusen, can you comment on this? Obviously, GAO has taken a look at all the government. Have you witnessed any stovepipes, any turf wars?

Mr. WILSHUSEN. I will say that there could be at certain times among the agencies, particularly early on. But I think DHS has done a pretty good job as well, once it was given the statutory authority to issue binding operational directives. In the past, if DHS said something, there could have been some conflicts with other sister agencies. But I think the way it has shaken out with the authorities given to DHS and the way DHS has exercised those authorities that some of the turf wars have been alleviated.

Chairman JOHNSON. One of the big issues with cyber, it is just complex. I use the analogy of "Gilligan's Island." On this island most of us are Gilligans. Not too many professors know how to make a battery out of a coconut. It is just the vast majority of people do not understand this. We use the device. We just had the hearing with Facebook. The vast majority of people claimed, clicking on "I accept the policies," had no idea. I think there is great awareness of how much of their private information is now available and is being used, being monetized. That is a problem.

I am going to ask my final question in two parts, and it is unfair, but I am going to ask you to give me a number anyway, because I did not do it on individual, but just overall I think we have made a great deal of progress in this incredibly complex environment. I think from this testimony I have been given a little more comfort. We are getting our act together, but it is difficult, it is complex, and the folks on offense are always going to be—I do not know how far ahead. My sense is over the last 7 years we are closing the gap.

One of the beauties of cyber defense is you do not have to build an expensive wall. It is code, and it can be really implemented at the speed of light. But, people are always on offense.

My final question is, 0 to 10, how far have we come in terms of implementing of what we need to implement, first of all, in government but also then in the private sector? Actually, let us start with the private sector. Madam Secretary, why don't you start? Zero to 10, how far has the private sector come in terms of cybersecurity and cyber defense?

Ms. MANFRA. Well, it is——

Chairman JOHNSON. By the way, what I should do is have you rate—like "Jeopardy?!" write down your answer. [Laughter.]

No, I mean it. Write down your answer first.

Mr. WILSHUSEN. Over what period of time——

Chairman JOHNSON. First on the private sector. OK, how far have we come, 0 to 10 in terms of enacting cybersecurity?

Mr. WILSHUSEN. Over what period of time?

Chairman JOHNSON. The last 7 years. Where do we need to go? It does not make any difference. Where do we need to go, if 10 is we have this nailed and we have the defense to really defend against any offense? First of all, in the private sector and then where are we in government? Do not be looking at each other's work. [Laughter.]

We really ought to have that theme song.

Secretary Manfra, so what is your answer? I will trust you to tell me.

Ms. MANFRA. I think if I could preface, it is hard to treat the private sector as a monolithic entity.

Chairman JOHNSON. Oh, even government. I know.

Ms. MANFRA. Just prefacing——

Chairman JOHNSON. It is a very unfair question. I got it. It gives me some indication though.

Ms. MANFRA. In talking about it in terms of how far we have come, I would probably give us, both the private sector and the government, in the 5 to 6 range. That is simply just because I believe that we have come a really long way. However, to truly—and I hope you will appreciate this. I talk a lot about getting the advantage back to the defenders, and being from Wisconsin, I believe defense wins championships, except for maybe last year. But other than that——

Chairman JOHNSON. You need a little offense every now and then.

Ms. MANFRA. You need a little bit of offense. But I really do believe that we can use the asymmetric advantage that the United States does have, which is a strong industry in, whether it is the financial sector or the Internet, we have a powerful industry, we have a powerful government. What remains is putting it all together. I think this is DHS' thing to own. We do not own it completely. We have a lot of other partners in this. But that is sort of why I would put us in that 5 to 6 range.

Chairman JOHNSON. OK. But actually pretty equal between government and private sector, not one ahead of the other?

Ms. MANFRA. It is different challenges, but I do think equal.

Chairman JOHNSON. Mr. Wilshusen.

Mr. WILSHUSEN. Senator Carper once referred to me as a "glass-half-empty" type of guy, so I am going to go with a little bit lower than Jeanette and probably go 3 and 4, and I actually think——

Chairman JOHNSON. Is that 3 government, 4 private sector?

Mr. WILSHUSEN. Actually, no. The other.

Chairman JOHNSON. OK.

Mr. WILSHUSEN. Flipping. I actually think government may be further along than——

Chairman JOHNSON. Greater awareness, you think?

Mr. WILSHUSEN. I think it is greater awareness, and it is greater guidance from up at the top and having the standards and the framework in place; whereas, it is more monolithic than you say with the private sector, which is very heterogeneous and has many different areas. I know that there are always—when we go out to look at the security, which is not often, but we do examine the security controls at certain private companies, either providing services to the Federal Government or others, we typical find just as many if not worse security at those companies than we do find at the agencies. We find pretty significant vulnerabilities at the agencies.

I would say generally I think government has probably a greater framework for its overall information security policies and standards than do the private sector.

Chairman JOHNSON. Mr. Rosenbach, are you a glass-half-full or glass-half-empty?

Mr. ROSENBACH. I price myself on being an optimist. maybe that is because I lived through like the last 8 years, seeing all this bad stuff happen. I actually think the private sector is closer to 7, maybe 7.5. That is primarily because the cybersecurity industry and the tech sector are moving very quickly, and there are a lot of options out there that mitigate——

Chairman JOHNSON. But not everyone in the private sector. I mean, there are a lot of people down near 0.

Mr. ROSENBACH. Yes, of course. I think the government is 5. If you said Department of Defense, I would say, OK, well, of course, we are better than everyone else. [Laughter.]

But that is easy to do when you can tell people what to do and you have a $700 billion budget. But, overall, I think the government is probably 5, and that includes government policy about national security decisions, when we will respond to stuff, when we will attribute things.

Chairman JOHNSON. I know that is a very unfair question and it is a very subjective answer, but it does give you some sort of feel. We have come a long way. I think it is just obvious. But we have quite a ways to go, and we cannot take our eye off the ball here. These are very serious problems we face, an enormous challenge.

Again, I want to thank all of you for your testimony, for indulging my lengthy questions here. I think this was an excellent hearing, and I just want to thank you.

With that, the hearing record will remain open for 15 days until May 9 at 5 p.m. for the submission of statements and questions for the record.

This hearing is adjourned.

[Whereupon, at 12:34 p.m., the Committee was adjourned.]

# APPENDIX

**Chairman Johnson's Opening Statement**
**"Mitigating America's Cybersecurity Risk"**
**Tuesday, April 24, 2018**

*As prepared for delivery:*

Cybersecurity is one of this Committee's top priorities. In the five previous hearings I have held examining this threat, we have explored the importance of information sharing and the need for liability protections, federal data breaches, and the cost burden of duplicative cybersecurity regulations. The Committee has passed legislation to bolster the Department of Homeland Security's cybersecurity capabilities, including the Federal Cybersecurity Enhancement Act, which codified DHS's EINSTEIN and Continuous Diagnostics and Mitigation programs to protect federal networks.

Cyberattacks targeting government agencies, private businesses, and individuals are increasing in frequency and scope, costing the U.S. economy an estimated $109 billion in 2016. It is critical for the United States to implement a strategy to deter malicious nation-state actors and cyber criminals. Such a strategy requires robust cyber defenses, post-cyberattack resilience, and, when necessary, the ability to retaliate forcefully.

The Department is assigned some of the federal government's most important cybersecurity responsibilities. DHS's programs provide defensive capabilities to federal agencies and private industry, respond to cyber incidents, and develop law enforcement capacity to investigate cybercrime. DHS is also at the forefront of the government's efforts to support the private sector and defend the nation's networks.

Today's hearing will examine how effective federal government programs implemented by DHS are at mitigating cybersecurity risk. We must ensure these programs are successful and able to defend both government and private sector networks. I look forward to hearing more about how the federal government can support those in the private sector who are on the front lines of the cyber conflict.

This hearing will also examine DHS's efforts to provide voluntary assistance to secure infrastructure, including to U.S. election systems. The midterm elections are fast approaching, and I am glad to see the Administration and DHS working diligently to engage with the states, election agencies, and election service providers.

I want to thank all of the witnesses for being here today, and I look forward to your testimony.

**U.S. Senate Committee on Homeland Security and Governmental Affairs**
**"Mitigating America's Cybersecurity Risk"**

**April 24, 2018**
**Ranking Member Claire McCaskill**

## Opening Statement

Thank you Mr. Chairman. I appreciate you holding this hearing.

Hardly a week goes by without some type of cyber incident dominating the headlines. As the United States and the world become more digitally connected, I suspect that trend will only continue.

Our government is a lot older than the Internet, so we have had to retrofit technology into existing government structures. But unlike a lot of issues that naturally fit into a single department or agency, cybersecurity and data protection affect all aspects of government. In the last few years, however, Congress, and in particular this Committee, have made a great deal of progress enhancing the federal government's ability to track and improve its cybersecurity.

We codified the Department of Homeland Security (DHS) to coordinate the operational security of federal systems. That included designating DHS as the hub for information sharing, running the intrusion prevention and detection programs that are now mandated throughout federal departments, leading asset response activities, and coordinating the protection of critical infrastructure. When necessary, DHS also has the unique authority to direct another agency to take certain steps to protect its systems.

While every department and agency is ultimately in charge of protecting its own systems, Congress has done a lot to make DHS the primary cyber coordinator for the civilian federal government. This hearing is an opportunity to assess how DHS is using the authorities Congress provided and if those tools are measurably improving agencies' awareness and security.

As I mentioned, part of DHS's responsibilities also include coordinating critical infrastructure protection, but the majority of critical infrastructure is not federally owned or operated. That is certainly the case with election systems, which are owned and operated by states and localities.

We all know that the Intelligence Community assessed with high confidence that Russia launched a campaign to influence the 2016 election, part of which aimed to undermine public faith in the U.S. democratic process. A component of that operation included attempts to hack into voter registration systems.

In the months before the election, DHS stepped up and offered cyber assistance to states that wanted help. And in the aftermath of the election, DHS designated election infrastructure as critical infrastructure, which enabled interested states and localities to jump toward the front of the line to receive that help.

In the roughly two years since this issue appeared on the radar of states and the federal government, DHS has made progress building relationships with election officials and associated organizations throughout the country, and in helping interested states and localities assess and improve the security of their voting systems. There have certainly been some bumps in the road, but I think DHS is on the right track. That said, I have serious reservations about our level of preparedness. Just last week, DHS Secretary Nielsen declined to express confidence in the country's election security, admitting only that there is increased awareness of the threat. I find that troubling.

Beyond that, I am concerned that this Administration has only been treating the symptoms of Russia's interference. U.S. policy towards Russia has been uneven at best, and at worst, I worry that we have done little if anything to actually change Russian behavior and stop them from trying to undermine our institutions and democracy.

I look forward to hearing our distinguished witnesses' assessments of our cyber and election security and how we can improve it in the future.

Thank you, Mr. Chairman.

Statement for the Record

Jeanette Manfra
Assistant Secretary
Office of Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
United States Senate
Committee on Homeland Security and Government Affairs

Regarding

Mitigating America's Cybersecurity Risk

April 24, 2018

Chairman Johnson, Ranking Member McCaskill, and members of the Committee, thank you for the opportunity to testify before you today. The Department of Homeland Security (DHS) serves a critical role in safeguarding and securing cyberspace, a core homeland security mission. The National Protection and Programs Directorate (NPPD) at DHS leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure. Last month, this Committee reported favorably on H.R. 2825, the *Department of Homeland Security Authorization Act* (as amended). This bill includes the language from H.R. 3359, the *Cybersecurity and Infrastructure Security Agency Act of 2017*. If enacted, this language would mature and streamline NPPD and rename our organization to reflect clearly our essential mission and our role in securing cyberspace. The Administration strongly supports establishing the Cybersecurity and Infrastructure Security Agency within DHS, and we will continue working with this Committee and the rest of the Senate to get the necessary legislation enacted.

NPPD is responsible for protecting civilian Federal government networks and collaborating with other Federal agencies, as well as State, local, tribal, and territorial governments, and the private sector to defend against cyber threats. We endeavor to enhance cyber threat information-sharing across the globe to stop cyber incidents before they start and help businesses and government agencies to protect their cyber systems and quickly recover should such an attack occur. By bringing together all levels of government, the private sector, international partners, and the public, we are taking action to protect against cybersecurity risks, improve our whole-of-government incident response capabilities, enhance information sharing of best practices and cyber threats, and to strengthen resilience.

**Threats**

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. Malicious cyber activity causes impacts to infrastructure across both the virtual and physical domains. We have recently experienced a turning point in the cyber domain, at least in the public consciousness. We have long been confronted with myriad attacks against our digital networks. Americans have seen advanced persistent threat actors, including hackers, cyber criminals, and nation states, increase the frequency and sophistication of these attacks. Our adversaries have been developing and using advanced cyber capabilities to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democracy.

Global cyber incidents, such as the "WannaCry" ransomware incident and the "NotPetya" malware incident in May and June 2017, respectively, are examples of malicious actors leveraging cyberspace to create disruptive effects and cause economic loss. These incidents exploited known vulnerabilities in software commonly used across the globe. Prior to these events, NPPD had already taken actions to help protect networks from similar types of attacks. Through requested vulnerability scanning, NPPD helped stakeholders identify vulnerabilities on their networks so they could be patched before incidents and attacks occur. Recognizing that not all users are able to install patches immediately, NPPD shared additional mitigation guidance to assist network defenders. As the incidents unfolded, NPPD led the Federal government's incident response efforts, working with our interagency partners, including providing situational awareness, information sharing, malware analysis, and technical assistance to affected entities.

In a series of incidents since at least May of last year, working with U.S. and international partners, DHS and FBI have identified Russian government actors targeting government entities and businesses in the energy, nuclear, water, aviation, and critical manufacturing sectors. DHS assesses that this campaign ultimately collected information pertaining to industrial control systems with the intent to gain access to industrial control systems environments. The intrusions have targeted two distinct categories of victims: staging and intended targets. In other words, through the Department's incident response actions, we have observed this advanced persistent threat actor target certain entities that then become pivot points, leveraging existing relationships between the initial victim and the intended targets to hide their activity, as part of a multi-stage intrusion campaign to gain access to networks of major, high-value assets that operate components of our Nation's critical infrastructure. Based on our analysis and observed indicators of compromise, DHS has confidence that this campaign is still ongoing, and threat actors are actively pursuing their ultimate long-term campaign objectives. DHS and the FBI continue to conduct incident response related to this activity and have published a joint technical alert to enable network defenders to identify and take action to reduce exposure to this malicious activity.

**Cybersecurity Priorities**

This Administration has prioritized protecting and defending our public and economic safety from the range of threats that exist today, including those emanating from cyberspace. Last year, the President signed Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This Executive Order set in motion a series of assessments and deliverables to understand how to improve our defenses and lower our risk to cyber threats. This order also emphasized the importance of accountability–clarifying that department and agency heads are responsible and will be held accountable for the security of their networks and systems. NPPD plays an important role in providing capabilities, services, and direction to Federal agencies.

Across the Federal Government, agencies have been implementing action plans to use the industry-standard National Institute of Standards and Technology (NIST) Cybersecurity Framework. Agencies are reporting to DHS and the Office of Management and Budget (OMB) on their cybersecurity risk mitigation and acceptance choices. In coordination with OMB, DHS is evaluating the totality of these Agency reports in order to comprehensively assess the adequacy of the Federal Government's overall cybersecurity risk management posture.

Although Federal agencies have primary responsibility for their own cybersecurity, DHS provides a common set of security tools that helps agencies manage their cyber risk. NPPD's assistance to Federal agencies includes (1) providing tools to safeguard civilian executive branch networks through the National Cybersecurity Protection System (NCPS), which includes "EINSTEIN" and Continuous Diagnostics and Mitigation (CDM) programs, (2) measuring and motivating agencies to implement policies, directives, standards, and guidelines, (3) serving as a hub for information sharing and incident reporting, and (4) providing operational and technical assistance, including threat information dissemination and risk and vulnerability assessments, as well as incident response services. NPPD's National Cybersecurity and Communications Integration Center (NCCIC) is the civilian government's hub for cybersecurity information sharing, asset incident response, and coordination for both critical infrastructure and the Federal government.

EINSTEIN refers to the Federal Government's suite of signature-based intrusion detection and prevention capabilities that protects agencies' unclassified networks at the perimeter of each agency. EINSTEIN provides situational awareness of civilian executive branch network traffic, so threats detected at one agency are shared with all others providing agencies with information and capabilities to more effectively manage their cyber risk. The Federal Government could not achieve such situational awareness through individual agency efforts alone.

Moving forward, leveraging existing investments, our non-signature based pilot efforts to move beyond current reliance on signatures are yielding positive results in the discovery of previously unidentified malicious activity. DHS is demonstrating the ability to capture data that can be rapidly analyzed for anomalous activity using technologies from commercial, government, and open sources. The pilot efforts are also defining the future operational needs for tactics, techniques, and procedures as well as the skill sets and personnel required to operationalize the non-signature based approach to cybersecurity.

State, local, tribal, and territorial governments are able to access intrusion detection and analysis services through the Multi-State Information Sharing and Analysis Center (MS-ISAC). MS-ISAC's service, called "Albert," closely resembles some EINSTEIN capabilities. While the current version of Albert cannot actively block known cyber threats, it does alert cybersecurity officials to an issue for further investigation. DHS worked closely with MS-ISAC to develop the program and considers MS-ISAC to be a principal conduit for sharing cybersecurity information with state and local governments.

EINSTEIN, the Federal Government's tool to address perimeter security, will not block every threat; therefore, it must be complemented with systems and tools working inside agency networks—as effective cybersecurity risk management requires a defense-in-depth strategy that cannot be achieved through only one type of tool. CDM program provides cybersecurity tools and integration services to all participating agencies to enable them to improve their respective security postures by reducing the attack surface of their networks as well as providing DHS with enterprise-wide visibility through a common federal dashboard.

CDM is helping us achieve two major advances for federal cybersecurity. First, agencies are gaining visibility, often for the first time, into the extent of cybersecurity risks across their entire network. With enhanced visibility, they can prioritize the mitigation of identified issues based upon their relative importance. Second, with the summary-level agency-to-federal dashboard feeds, the NCCIC will be able to identify systemic risks across the civilian executive branch more effectively and closer to real-time. For example, the NCCIC currently tracks government-wide progress in implementing critical patches via agency self-reporting and manual data calls. CDM will transform this, enabling the NCCIC to immediately view the prevalence of a given software product or vulnerability across the federal government so that the NCCIC can provide agencies with timely guidance on their risk exposure and recommended mitigation steps. Effective cybersecurity requires a robust measurement regime, and robust measurement requires valid and timely data. CDM will provide this baseline of cybersecurity risk data to drive improvement across the civilian executive branch.

DHS conducts a number of activities to measure agencies' cybersecurity practices and works with agencies to improve risk management practices. The Federal Information Security Modernization Act of 2014 (FISMA) provided the Secretary of Homeland Security with the authority to develop and oversee implementation of Binding Operational Directives (BOD) to agencies. In 2016, the Secretary issued a BOD on securing High Value Assets, or those assets, federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to U.S. national security interests, foreign relations, the economy, or to the public confidence, civil liberties, or public health and safety of the American people. NPPD works with interagency partners to prioritize High Value Assets for assessment and remediation activities across the federal government. For instance, NPPD conducts security architecture reviews on these High Value Assets to help agencies assess their network architecture and configurations.

As part of the effort to secure High Value Assets, DHS conducts in-depth vulnerability assessments of prioritized agency assets to determine how an adversary could penetrate a system, move around an agency's network to access sensitive data, and exfiltrate such data without being detected. These assessments include services such as penetration testing, wireless security analysis, and "phishing" evaluations in which DHS hackers send emails to agency personnel and test whether recipients click on potentially malicious links. DHS has focused these assessments on federal systems that may be of particular interest to adversaries or support uniquely significant data or services. These assessments provide system owners with recommendations to address identified vulnerabilities. DHS provides these same assessments, on a voluntary basis upon request, to private sector and State, local, Territorial, and Tribal partners. DHS also works with the General Services Administration to ensure that contractors can provide assessments that align with our HVA initiative to agencies.

Another BOD issued by the Secretary directs civilian agencies to promptly patch known vulnerabilities on their Internet-facing systems that are most at risk from their exposure. The NCCIC conducts cyber hygiene scans to identify vulnerabilities in agencies' internet-accessible devices and provides mitigation recommendations. Agencies have responded quickly in implementing the Secretary's BOD and have sustained this progress. When the Secretary issued this directive, NPPD identified more than 360 "stale" critical vulnerabilities across federal civilian agencies, which means the vulnerabilities had been known for at least 30 days and remained unpatched. Since December 2015, NPPD has identified an average of less than 40 critical vulnerabilities at any given time, and agencies have addressed those vulnerabilities rapidly once they were identified. By conducting vulnerability assessments and security architecture reviews, NPPD is helping agencies find and fix vulnerabilities and secure their networks before an incident occurs.

In addition to efforts to protect government networks, Executive Order 13800 continues to examine how the government and industry work together to protect our nation's critical infrastructure, prioritizing deeper, more collaborative public-private partnerships in threat assessment, detection, protection, and mitigation. In collaboration with civilian, defense, and intelligence agencies, we are identifying authorities and capabilities that agencies could employ, soliciting input from the private sector, and developing recommendations to support the cybersecurity efforts of those critical infrastructure entities at greatest risk of attacks that could result in catastrophic impacts. DHS coordinates closely with the Sector Specific Agencies across all 16 critical infrastructure sectors by leveraging their sector expertise to improve cybersecurity resiliency and risk management.

For instance, by sharing information quickly and widely, we help all partners block cyber threats before damaging incidents occur. Equally important, the information we receive from partners helps us identify emerging risks and develop effective protective measures.

Congress authorized the NCCIC as the civilian hub for sharing cyber threat indicators and defensive measures with and among federal and non-federal entities, including the private sector. As required by the Cybersecurity Act of 2015, we established a capability, known as Automated Indicator Sharing (AIS), to automate our sharing of cyber threat indicators in real-time. AIS protects the privacy and civil liberties of individuals by narrowly tailoring the information shared to that which is necessary to characterize identified cyber threats, consistent with longstanding DHS policy and the requirements of the Act. AIS is a part of the Department's effort to create an environment in which as soon as a company or federal agency observes an attempted compromise, the indicator is shared in real time with all of our partners, enabling them to protect themselves from that particular threat. This real-time sharing capability can limit the scalability of many attack techniques, thereby increasing the costs for adversaries and reducing the impact of malicious cyber activity. An ecosystem built around automated sharing and network defense-in-depth should enable organizations to detect and thwart the most common cyber-attacks, freeing their cybersecurity staff to concentrate on the novel and sophisticated attacks. More than 129 agencies and private sector partners have connected to the AIS capability. Notably, partners such as information sharing and analysis organizations and computer emergency response teams further share with or protect their customers and stakeholders, significantly expanding the impact of this capability. AIS is still a new capability and we expect the volume of threat indicators shared through this system to substantially increase as the technical standards, software, and hardware supporting the system continue to be refined and put into full production. This information sharing environment will become more robust and effective as more indicators are shared from other federal agencies; State, local, Territorial, and Tribal governments; and the private sector.

Another part of the Department's overall information sharing effort is to provide federal network defenders with the necessary context regarding cyber threats to prioritize their efforts and inform their decision making. DHS's Office of Intelligence and Analysis has collocated analysts within the NCCIC responsible for continuously assessing the specific threats to federal networks using traditional all source methods and indicators of malicious activity so that the NCCIC can share with federal network defenders. Analysts and personnel from the Departments of Energy, the Treasury, Health and Human Services, and Defense join the FBI and others who are also collocated within the NCCIC and working together to understand the threats and share information with their sector stakeholders, pursuant to NPPD policies that provide appropriate privacy, civil liberties and confidentiality protections.

**Mitigating Cyber Risks**

We continue to adapt to the evolving risks to critical infrastructure, and prioritize our services to mitigate those risks. For instance, the Department recently took action regarding specific products which present a risk to federal information systems.

After careful consideration of available information and consultation with interagency partners, BOD 17-01 was issued that directed Federal Executive Branch departments and agencies to take actions related to the use or presence of information security products, solutions, and services supplied directly or indirectly by AO Kaspersky Lab or related entities. The BOD called on departments and agencies to identify any use or presence of Kaspersky products on their information systems in the next 30 days, to develop detailed plans to remove and discontinue present and future use of the products within 60 days, and at 90 days from the date of the directive, unless directed otherwise by DHS based on new information, to begin to implement the agency plans to discontinue use and remove the products from federal information systems. This action is based on the information security risks presented by the use of Kaspersky products on federal IT systems.

The Department provided an opportunity for Kaspersky to submit a written response addressing the Department's concerns or to mitigate those concerns, and Kaspersky submitted a written response. The Department wanted to ensure that the company had a full opportunity to provide any evidence, materials, or data that may be relevant. This opportunity was also available to any other entity that claimed its commercial interests will be directly impacted by the directive.

While the information and communications technology supply chain is not the source of all cyber risk, it presents an opportunity for creation of threats and vulnerabilities. Commercial technology is ubiquitous in federal networks, even those that handle the most sensitive information and support essential functions of the government. DHS—through its work with the Department of Defense and the intelligence community to identify key supply chain risks—has established a Cyber Supply Chain Risk Management initiative. Due to the increasing connectivity of the world and the growing sophistication of threats, this initiative will identify and mitigate supply chain threats and vulnerabilities related to High Value Assets.

**Election Security**

NPPD is committed to ensuring a coordinated response from DHS and its federal partners to plan for, prepare for, and mitigate risk to election infrastructure. We understand that working with election infrastructure stakeholders is essential to ensuring a more secure election. Based on our assessment of activity observed in the 2016 elections, NPPD and our stakeholders are increasing awareness of potential vulnerabilities and providing capabilities to enhance the security of U.S. election infrastructure as well as that of our democratic allies.

As mentioned before, under the Constitution and our system of laws, federal elections are administered by state and local election officials in thousands of jurisdictions. Security awareness for election officials did not begin in 2016, State and local election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections. In partnering with these officials through both new and existing, ongoing engagements, NPPD is working to provide value-added–yet voluntary–services to support their efforts to secure elections.

This year our Nation is in the midst of primary and special elections as well as the general election in November. We have been working with election officials in all states to enhance the security of their elections by offering support and by establishing essential lines of communications at all levels–public and private–for reporting both suspicious cyber activity and incidents. This information sharing is critical and our goal is to enhance transparency and have visibility of aggregated elections-related cybersecurity efforts. We are also working with election officials, vendors, the Election Assistance Commission (EAC), and NIST to characterize risk to election systems and ensure appropriate mitigations are understood and available in the marketplace. As a part of this process, we work with these stakeholders to recommend best practices to ensure a secure and verifiable vote.

Over the course of the last year, DHS has made tremendous strides and has been committed to working collaboratively with those on the front lines of administering our elections—state and local election officials and the vendor community—to secure election infrastructure from risks. The establishment of government and sector coordinating councils will build the foundations for this enduring partnership not only in 2018, but for future elections as well. We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. However, we recognize that there is a significant technology deficit across State and local governments, and State and local election systems, in particular. It will take significant and continual investment to ensure that systems are upgraded and secure or vulnerable systems are retired.

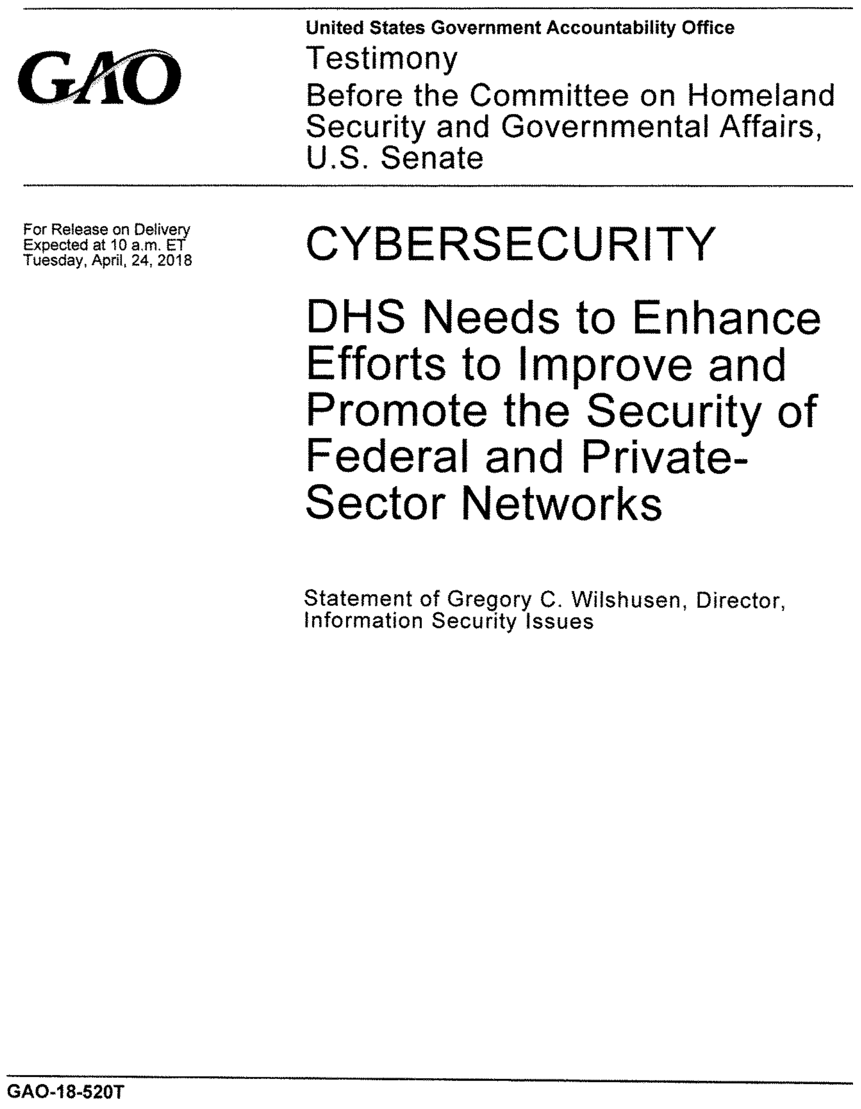
We recognize the fundamental link between public trust in our election infrastructure and the confidence the American public places in basic democratic functions. Ensuring the security of our electoral process is a vital national interest and one of our highest priorities at DHS. Our voting infrastructure is diverse, subject to local control, and has many checks and balances. As the threat environment evolves, DHS will continue to work with federal agencies, state and local partners, and private sector entities to enhance our understanding of the threat; and to make essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

**Conclusion**

In the face of increasingly sophisticated threats, NPPD stands on the front lines of the federal government's efforts to defend our nation's critical infrastructure from natural disasters, terrorism and adversarial threats, and technological risk such as those caused by cyber threats. Our infrastructure environment today is complex and dynamic with interdependencies that add to the challenge of securing and making it more resilient. Technological advances have introduced the "Internet of Things" and cloud computing, offering increased access and streamlined efficiencies, while increasing our footprint of access points that could be leveraged by adversaries to gain unauthorized access to networks. As our nation continues to evolve and new threats emerge, we must integrate cyber and physical risk in order to understand how to effectively secure it. Expertise around cyber-physical risk and cross-sector critical infrastructure interdependencies is where NPPD brings unique expertise and capabilities.

We must ensure that NPPD is appropriately organized to address cybersecurity threats both now and in the future, and we appreciate this Committee's leadership in working to establish the Cybersecurity and Infrastructure Security Agency. As the Committee considers these issues, we are committed to working with Congress to ensure that this effort is done in a way that cultivates a safer, more secure and resilient Homeland.

Thank you for the opportunity to testify, and I look forward to any questions you may have.



**United States Government Accountability Office**

Testimony
Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10 a.m. ET
Tuesday, April, 24, 2018

# CYBERSECURITY

# DHS Needs to Enhance Efforts to Improve and Promote the Security of Federal and Private-Sector Networks

Statement of Gregory C. Wilshusen, Director, Information Security Issues

# GAO Highlights

Highlights of GAO-18-520T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

## Why GAO Did This Study

The emergence of increasingly sophisticated threats and continuous reporting of cyber incidents underscores the continuing and urgent need for effective information security. GAO first designated information security as a government-wide high-risk area in 1997. GAO expanded the high-risk area to include the protection of cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.

Federal law and policy provide DHS with broad authorities to improve and promote cybersecurity. DHS plays a key role in strengthening the cybersecurity posture of the federal government and promoting cybersecurity of systems supporting the nation's critical infrastructures.

This statement highlights GAO's work related to federal programs implemented by DHS that are intended to improve federal cybersecurity and cybersecurity over systems supporting critical infrastructure. In preparing this statement, GAO relied on a body of work issued since fiscal year 2016 that highlighted, among other programs, DHS's NCPS, national integration center activities, and cybersecurity workforce assessment efforts.

## What GAO Recommends

Since fiscal year 2016, GAO has made 29 recommendations to DHS to enhance the capabilities of NCPS, establish metrics and methods for evaluating performance, and fully assess its cybersecurity workforce, among other things. As of April 2018, DHS had not demonstrated that it had fully implemented most of the recommendations.

View GAO-18-520T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

April 24, 2018

# CYBERSECURITY

## DHS Needs to Enhance Efforts to Improve and Promote the Security of Federal and Private-Sector Networks

## What GAO Found

In recent years, the Department of Homeland Security (DHS) has acted to improve and promote the cybersecurity of federal and private-sector computer systems and networks, but further improvements are needed. Specifically, consistent with its statutory authorities, DHS has made important progress in implementing programs and activities that are intended to mitigate cybersecurity risks on the computer systems and networks supporting federal operations and our nation's critical infrastructure. For example, the department has:

- provided limited intrusion detection and prevention capabilities to entities across the federal government;
- issued cybersecurity related binding operational directives to federal agencies;
- served as the federal-civilian interface for sharing cybersecurity related information with federal and nonfederal entities;
- promoted the use of the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*; and
- partially assessed its cybersecurity workforce.

Nevertheless, the department has not taken sufficient actions to ensure that it successfully mitigates cybersecurity risks on federal and private-sector computer systems and networks. For example, GAO reported in 2016 that DHS's National Cybersecurity Protection System (NCPS) had only partially met its stated system objectives of detecting and preventing intrusions, analyzing malicious content, and sharing information. GAO recommended that DHS enhance capabilities, improve planning, and support greater adoption of NCPS.

In addition, although the department's National Cybersecurity and Communications Integration Center generally performed required functions such as collecting and sharing cybersecurity related information with federal and non-federal entities, GAO reported in 2017 that the center needed to evaluate its activities more completely. For example, the extent to which the center had performed its required functions in accordance with statutorily defined implementing principles was unclear, in part, because the center had not established metrics and methods by which to evaluate its performance against the principles. Further, in its role as the lead federal agency for collaborating with eight critical infrastructure sectors including the communications and dams sectors, DHS had not developed metrics to measure and report on the effectiveness of its cyber risk mitigation activities or on the cybersecurity posture of the eight sectors.

GAO reported in 2018 that DHS had taken steps to assess its cybersecurity workforce; however, it had not identified all of its cybersecurity positions and critical skill requirements.

Until DHS fully and effectively implements its cybersecurity authorities and responsibilities, the department's ability to improve and promote the cybersecurity of federal and private-sector networks will be limited.

Chairman Johnson, Ranking Member McCaskill, and Members of the Committee:

Thank you for the opportunity to appear at today's hearing on how federal government programs implemented by the Department of Homeland Security (DHS) are mitigating cybersecurity risk for federal and private-sector networks. As recent cyberattacks have illustrated, the need for robust and effective cybersecurity has never been greater.

At your request, I will provide an overview of our work issued since 2016 related to federal programs implemented by DHS that are intended to improve federal cybersecurity and cybersecurity over systems supporting critical infrastructure. My statement highlights our cybersecurity audit findings and recommendations, including recommendations for improving DHS's implementation of its cybersecurity authorities and management of federal programs to mitigate cyber risks on networks.

In developing this testimony, we relied on our previous reports, as well as information provided by DHS on its actions in response to our previous recommendations.[1] We also considered information security related information that the Office of Management and Budget reported to Congress for fiscal year 2017.[2] A more detailed discussion of the

[1] GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 15, 2018); GAO, *Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*, GAO-18-175 (Washington, D.C.: Feb. 6, 2018); GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, GAO-17-549 (Washington, D.C.: Sept. 28, 2017); GAO, *Cybersecurity: Federal Efforts Are Under Way That May Address Workforce Challenges*, GAO-17-533T (Washington, D.C.: Apr. 4, 2017); GAO, *Information Security: DHS Needs to Continue to Advance Initiatives to Protect Federal Systems*, GAO-17-518T (Washington, D.C.: Mar. 28, 2017); GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017); GAO, *Cybersecurity: Actions Needed to Strengthen U.S. Capabilities*, GAO-17-440T (Washington, D.C.: Feb. 14, 2017); GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely*, GAO-17-163 (Washington, D.C.: Feb. 1, 2017); GAO, *Federal Information Security: Actions Needed to Address Challenges*, GAO-16-885T (Washington, D.C.: Sept. 19, 2016); GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016); GAO, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, GAO-16-152 (Washington, D.C.: Dec. 17, 2015); and GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015).

[2] Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2017*, (Washington, D.C.: Mar. 2018).

objectives, scope, and methodology for this work is included in each of the reports that are cited throughout this statement.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a reasonable basis for our findings and conclusions based on our audit objectives.

## Background

Federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications networks, and financial services—are dependent on computerized (cyber) information systems and electronic data to process, maintain, and report essential information, and to operate and control physical processes. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. Ineffective security controls to protect these systems and data could have a significant impact on a broad array of government operations and assets.

Yet, computer networks and systems used by federal agencies are often riddled with security vulnerabilities—both known and unknown. These systems are often interconnected with other internal and external systems and networks, including the Internet, thereby increasing the number of avenues of attack and expanding their attack surface.

Furthermore, safeguarding federal computer systems has been a long-standing concern. This year marks the 21st anniversary of when GAO first designated information security as a government-wide high-risk area in 1997.[3] We expanded this high-risk area to include safeguarding the

[3] GAO designates agencies and program areas as high risk due to their vulnerability to fraud, waste, abuse, and mismanagement, or when they are most in need of transformation.

systems supporting our nation's critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.[4]

Over the last several years, we have made about 2,500 recommendations to agencies aimed at improving the security of federal systems and information. These recommendations identified actions for agencies to take to strengthen their information security programs and technical controls over their computer networks and systems. Nevertheless, many agencies continue to be challenged in safeguarding their information systems and information, in part because they have not implemented many of these recommendations. As of March 2018, about 885 of our prior information security-related recommendations had not been implemented.

## Federal Law and Policy Provide DHS with Broad Authorities to Improve and Promote Cybersecurity

DHS has broad authorities to improve and promote cybersecurity of federal and private-sector networks. The federal laws and policies that underpin these authorities include the following:

- **The Federal Information Security Modernization Act (FISMA) of 2014**[5] clarified and expanded DHS's responsibilities for assisting with the implementation of, and overseeing, information security at federal agencies. These responsibilities include requirements to:
  - develop, issue, and oversee agencies' implementation of binding operational directives to agencies, including directives for incident reporting, contents of annual agency reports, and other operational requirements;
  - monitor agencies' implementation of information security policies and practices; and
  - provide operational and technical assistance to agencies, including by operating the federal information security incident center, deploying technology to continuously diagnose and mitigate threats, and conducting threat and vulnerability assessments of systems.

[4] GAO-17-317.

[5] The *Federal Information Security Modernization Act of 2014* was enacted as Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), and amended chapter 35 of Title 44, U.S. Code.

- **The Homeland Security Cybersecurity Workforce Assessment Act of 2014,** among other things, requires DHS to assess its cybersecurity workforce.[6] In this regard, the Secretary of Homeland Security is to identify all positions in DHS that perform cybersecurity functions and to identify cybersecurity work categories and specialty areas of critical need.
- **The National Cybersecurity Protection Act of 2014**[7] codified the role of the National Cybersecurity and Communications Integration Center (NCCIC)—a center established by DHS in 2009—as the federal civilian interface for sharing information concerning cybersecurity risks, incidents, analysis, and warnings to federal and non-federal entities, including owners and operators of information systems supporting critical infrastructure.
- **The Cybersecurity Act of 2015**, among other things, sets forth authority for enhancing the sharing of cybersecurity-related information among federal and non-federal entities.[8] The act gives DHS's NCCIC responsibility for implementing this information sharing authority. The act also requires DHS to:
    - Jointly develop with other specified agencies and submit to Congress, procedures for sharing federal cybersecurity threat information and defensive measures with federal and non-federal entities.
    - Deploy, operate, and maintain capabilities to prevent and detect cybersecurity risks in network traffic traveling to or from an agency's information system. DHS is to make these capabilities available for use by any agency. In addition, the act requires DHS to improve intrusion detection and prevention capabilities, as appropriate, by regularly deploying new technologies and modifying existing technologies.
- **Long-standing federal policy** as promulgated by a presidential policy directive, executive orders, and the National Infrastructure

[6] *The Homeland Security Cybersecurity Workforce Assessment Act of 2014* was enacted as section 4 of the *Border Patrol Agent Pay Reform Act of 2014*, Pub. L. No. 113-277 § 4,128 Stat. 2995, 3008-3010 (Dec. 18, 2014); 6 U.S.C. § 146 note.

[7] Pub. L. No. 113-282 (Dec. 18, 2014).

[8] The *Cybersecurity Act of 2015* was enacted into law as Division N of the *Consolidated Appropriations Act, 2016*, Pub. L. No. 114-113, 129 Stat. 2935-2985 (Dec. 18, 2015).

Protection Plan have designated DHS as a lead federal agency for coordinating, assisting, and sharing information with the private-sector to protect critical infrastructure from cyber threats.[9]

## DHS Has Acted to Improve and Promote the Cybersecurity of Federal and Private-Sector Computer Systems, but Further Improvements Are Needed

We have reviewed several federal programs and activities implemented by DHS that are intended to mitigate cybersecurity risk for the computer systems and networks supporting federal operations and our nation's critical infrastructure. These programs and activities include deploying the National Cybersecurity Protection System, providing continuous diagnostic and mitigation services, issuing binding operational directives, sharing information through the National Cybersecurity and Communications Integration Center, promoting adoption of a cybersecurity framework, and assisting private-sector partners with cyber risk mitigation activities. We also examined DHS's efforts to assess its cybersecurity workforce. DHS has made important progress in implementing these programs and activities. However, the department needs to take additional actions to ensure that it successfully mitigates cybersecurity risks on federal and private-sector computer systems and networks.

### DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System

DHS is responsible for operating its National Cybersecurity Protection System (NCPS), operationally known as EINSTEIN. NCPS is intended to provide intrusion detection and prevention capabilities to entities across

[9] The White House, *Critical Infrastructure Security and Resilience,* Presidential Policy Directive 21 (Washington, D.C.: Feb. 2013); The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* Exec. Order No. 13800, 82 Fed Reg. 22391 (Washington, D.C.: May 11, 2017); The White House, *Improving Critical Infrastructure Cybersecurity*, Exec. Order No. 13636, 78 Fed Reg. 11739, Vol.78, No. 33 (Feb. 19, 2013); Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: 2013); and Department of Homeland Security, Homeland Security Presidential Directive 7: *Critical Infrastructure Identification, Prioritization, and Protection*, (Dec. 17, 2003).

the federal government. It also is intended to provide DHS with capabilities to detect malicious traffic traversing federal agencies' computer networks, prevent intrusions, and support data analytics and information sharing.

In January 2016, we reported that the NCPS was partially, but not fully, meeting most of its stated four system objectives:[10]

- **Intrusion detection:** We noted that NCPS provided DHS with a limited ability to detect potentially malicious activity entering and exiting computer networks at federal agencies. Specifically, NCPS compared network traffic to known patterns of malicious data, or "signatures," but did not detect deviations from predefined baselines of normal network behavior. In addition, the system did not monitor several types of network traffic and its "signatures" did not address threats that exploited many common security vulnerabilities and, thus was not effective in detecting certain types of malicious traffic.
- **Intrusion prevention:** The capability of NCPS to prevent intrusions (e.g., blocking an e-mail determined to be malicious) was limited to the types of network traffic that it monitored. For example, the intrusion prevention function monitored and blocked e-mail. However, it did not address malicious content from other types of network traffic.
- **Analytics:** NCPS supports a variety of data analytical tools, including a centralized platform for aggregating data and a capability for analyzing the characteristics of malicious code. In addition, DHS had further enhancements to this capability planned through 2018.
- **Information sharing:** DHS had not developed most of the planned functionality for NCPS's information-sharing capability, and requirements had only recently been approved. Moreover, we noted that agencies and DHS did not always agree about whether notifications of potentially malicious activity had been sent or received, and agencies had mixed views about the usefulness of these notifications. Further, DHS did not always solicit—and agencies did not always provide—feedback on the notifications.

We recommended that DHS take nine actions to enhance NCPS's capabilities for meeting its objectives, better define requirements for

[10] GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016).

future capabilities, and develop network routing guidance. The department agreed with our recommendations; however, as of April 2018, it had not fully implemented 8 of the 9 recommendations. As part of a review mandated by the Federal Cybersecurity Enhancement Act of 2015, we are currently examining DHS's efforts to improve its intrusion detection and prevention capabilities.

## DHS Needs to Continue to Advance CDM Program to Protect Federal Systems

The Continuous Diagnostics and Mitigation (CDM) program was established to provide federal agencies with tools and services that have the intended capability to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at agency and government-wide levels. These tools include sensors that perform automated scans or searches for known cyber vulnerabilities, the results of which can feed into a dashboard that alerts network managers and enables the agency to allocate resources based on the risk.

DHS, in partnership with, and through the General Services Administration, established a government-wide acquisition vehicle for acquiring CDM capabilities and tools. The CDM blanket purchase agreement is available to federal, state, local, and tribal government entities for acquiring these capabilities.

There are three phases of CDM implementation and the dates for implementing Phase 2 and Phase 3 appear to be slipping:

**Phase 1:** This phase involves deploying products to automate hardware and software asset management, configuration settings, and common vulnerability management capabilities. According to the *Cybersecurity Strategy and Implementation Plan*, DHS purchased Phase 1 tools and integration services for all participating agencies in fiscal year 2015.[11]

**Phase 2:** This phase intends to address privilege management and infrastructure integrity by allowing agencies to monitor users on their networks and to detect whether users are engaging in unauthorized

[11] Office of Management and Budget, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, OMB Memorandum M-16-04 (Washington, D.C.: Oct. 30, 2015). CSIP identified objectives, key actions, responsibilities, and timeframes for completing actions that were intended to strengthen cybersecurity at federal civilian agencies.

activity. According to the *Cybersecurity Strategy and Implementation Plan*, DHS was to provide agencies with additional Phase 2 capabilities throughout fiscal year 2016, with the full suite of CDM phase 2 capabilities delivered by the end of that fiscal year. However, according to the Office of Management and Budget's (OMB) FISMA Annual Report to Congress for Fiscal Year 2017, the CDM program began deploying Phase 2 tools and sensors during fiscal year 2017.[12]

**Phase 3:** According to DHS, this phase is intended to address boundary protection and event management throughout the security life cycle. It focuses on detecting unusual activity inside agency networks and alerting security personnel. The agency had planned to provide 97 percent of federal agencies the services they need for CDM Phase 3 in fiscal year 2017. However, according to OMB's FISMA report for fiscal year 2017, the CDM program will continue to incorporate additional capabilities, including Phase 3, in fiscal year 2018.

In May 2016,[13] we reported that most of the 18 agencies covered by the CFO Act that had high-impact systems were in the early stages of implementing CDM.[14] All 17 of the civilian agencies that we surveyed indicated they had developed their own strategy for information security continuous monitoring.[15] Additionally, according to the survey responses, 14 of the 17 civilian agencies had deployed products to automate hardware and software asset configuration settings and common vulnerability management.

[12] Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2017*, (Washington, D.C.: 2018).

[13] GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016). We surveyed the 18 agencies covered by the Chief Financial Officers (CFO) Act that reported having high-impact systems on a variety of information security-related issues including their implementation of government-wide security initiatives such as the CDM program.

[14] High-impact systems are those where the loss of the confidentiality, integrity, or availability of the information or information system could be expected to have a severe or catastrophic adverse effect on organizations operations, assets, or personnel. For example, it might cause the organization to be unable to perform one or more of its primary functions or result in a major financial loss. Of the 24 CFO Act agencies, 18 reported having high-impact systems at the time of our review.

[15] The Department of Defense, one of the 18 agencies with high-impact systems, is not required to participate in the CDM program.

Further, more than half of these agencies noted that they had leveraged products/tools provided through the General Services Administration's acquisition vehicle. However, only 2 of the 17 agencies reported that they had completed installation of agency and bureau/component-level dashboards and monitored attributes of authorized users operating in their agency's computing environment. Agencies noted that expediting the implementation of the CDM phases could be of benefit to them in further protecting their high-impact systems.

Subsequently, in March 2017, we reported that the effective implementation of the CDM tools and capabilities can assist agencies in overcoming the challenges of securing their information systems and information.[16] We noted that our audits often identify insecure configurations, unpatched or unsupported software, and other vulnerabilities in agency systems. Thus, the tools and capabilities available under the CDM program, when effectively used by agencies, can help them to diagnose and mitigate vulnerabilities to their systems. We reported that, by continuing to make these tools and capabilities available to federal agencies, DHS can also have additional assurance that agencies are better positioned to protect their information systems and information.

## Other DHS Services Are Available to Help Protect Systems but Are Not Always Used by Agencies

Beyond the NCPS and CDM programs, DHS also provides a number of services that could help agencies protect their information systems. Such services include, but are not limited to:

- *US-CERT monthly operational bulletins*, which are intended to provide senior federal government information security officials and staff with actionable information to improve their organization's cybersecurity posture based on incidents observed, reported, or acted on by DHS and US-CERT.
- *CyberStat reviews*, which are in-depth sessions attended by National Security Staff, as well as officials from OMB, DHS, and an agency to discuss that agency's cybersecurity posture and opportunities for collaboration. According to OMB, these interviews are face-to-face,

[16] GAO, Information Security: DHS Needs to Continue to Advance Initiatives to Protect Federal Systems, GAO-17-518T (Washington, D.C.: Mar. 28, 2017).

evidence-based meetings intended to ensure agencies are accountable for their cybersecurity posture. The sessions are intended to assist the agencies in developing focused strategies for improving their information security posture in areas where there are challenges.

- *DHS Red and Blue Team exercises* that are intended to provide services to agencies for testing their systems with regard to potential attacks. A Red Team emulates a potential adversary's attack or exploitation capabilities against an agency's cybersecurity posture. The Blue Team defends an agency's information systems when the Red Team attacks, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group.

In May 2016, we reported that, although participation in these services varied among the 18 agencies we surveyed, most of those that chose to participate reported that they generally found these services to be useful in aiding the cybersecurity protection of their high-impact systems.[17] Specifically,

- 15 of 18 agencies reported that they participated in US-CERT monthly operational bulletins, and most said they found the service very or somewhat useful.
- All 18 agencies reported that they participated in the CyberStat reviews, and most said they found the service very or somewhat useful.
- 9 of 18 agencies reported that they participated in DHS' Red/Blue team exercises, and most said they found the exercises to be very or somewhat useful.

Half of the 18 agencies in our survey reported that they wanted an expansion of federal initiatives and services to help protect their high-impact systems. For example, these agencies noted that expediting the implementation of CDM phases, sharing threat intelligence information, and sharing attack vectors, could be of benefit to them in further protecting their high-impact systems. We believe that by continuing to make these services available to agencies, DHS will be better able to assist agencies in strengthening the security of their information systems.

[17] See GAO-16-501.

## DHS Has Issued Binding Operational Directives to Federal Agencies

FISMA authorizes DHS to develop and issue binding operational directives to federal agencies and oversee their implementation by agencies. The directives are compulsory and require agencies to take specific actions that are intended to safeguard federal information and information systems from a known threat, vulnerability, or risk.

In September 2017, we reported[18] that DHS had developed and issued four binding operational directives as of July 2017, instructing agencies to:

- mitigate critical vulnerabilities discovered by DHS's NCCIC through its scanning of agencies' Internet-accessible systems;[19]
- participate in risk and vulnerability assessments as well as DHS security architecture assessments conducted on agencies' high-value assets;[20]
- address several urgent vulnerabilities in network infrastructure devices identified in a NCCIC analysis report within 45 days of the directive's issuance;[21] and
- report cyber incidents and comply with annual FISMA reporting requirements.[22]

Since July 2017, DHS has issued two additional binding operational directives instructing agencies to:

- identify and remove the presence of any information security products developed by AO Kaspersky Lab on their information systems and discontinue the use of such products;[23] and

[18] GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, GAO-17-549 (Washington, D.C.: Sept. 28, 2017).

[19] Department of Homeland Security, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems*, BOD-15-01 (Washington, D.C.: May 21, 2015).

[20] Department of Homeland Security, *Securing High Value Assets*, BOD-16-01 (Washington, D.C.: June 9, 2016).

[21] Department of Homeland Security, *Threat to Network Infrastructure Devices*, BOD-16-02 (Washington, D.C.: Sept. 27, 2016).

[22] Department of Homeland Security, *2016 Agency Cybersecurity Reporting Requirements,* BOD-16-03 (Washington, D.C.: Oct. 17, 2016).

- enhance e-mail by, among other things, removing certain insecure protocols, and ensure public facing web sites provide services through a secure connection.[24]

We plan to initiate work later this year to identify and assess DHS's process for developing and overseeing agencies' implementation of binding operational directives.

## DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely

In February 2017, we reported that NCCIC had taken steps to perform each of its 11 statutorily required cybersecurity functions,[25] such as being a federal civilian interface for sharing cybersecurity-related information with federal and nonfederal entities.[26] NCCIC managed several programs that provided data used in developing 43 products and services that the center made available to its customers in the private-sector; federal, state, local, tribal and territorial government entities; and other partner organizations. For example, NCCIC issued indicator bulletins, which could contain information related to cyber threat indicators, defensive measures, and cybersecurity risks and incidents, and helped to fulfill its function to coordinate the sharing of such information across the government. Respondents to a survey that we administered to NCCIC's customers varied in their reported use of NCCIC's products but had generally favorable views of the center's activities.

The National Cybersecurity Protection Act also required NCCIC to carry out its functions in accordance with nine implementing principles, to the extent practicable. However, as we reported, the extent to which NCCIC

[23] Department of Homeland Security, *Removal of Kaspersky-Branded Products*, BOD-17-01 (Washington, D.C.: Sept. 13, 2017).

[24] Department of Homeland Security, *Enhance Email and Web Security*, BOD-18-01 (Washington, D.C.: Oct. 16, 2017).

[25] The National Cybersecurity Protection Act of 2014 requires NCCIC to share information and enable real-time actions to address cybersecurity risks and incidents at federal and non-federal entities, and adhere to nine principles when doing so. The Cybersecurity Act of 2015 added two more functions, for a total of 11 cybersecurity functions that the center is to perform.

[26] GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely*, GAO-17-163 (Washington, D.C.: Feb. 1, 2017).

adhered to the 9 principles when performing the functions was unclear because the center had not yet determined the applicability of the principles to all 11 functions. It also had not established metrics and methods by which to evaluate its performance against the principles.

We also identified several impediments to NCCIC performing its cybersecurity functions more efficiently. For example, the center did not have a centralized system for tracking security incidents and, as a result, could not produce a report on the status of all incidents reported to the center. In addition, the center did not keep current and reliable customer information and was unable to demonstrate that it had contact information for all owners and operators of the most critical cyber-dependent infrastructure assets.

We made nine recommendations to DHS for enhancing the effectiveness and efficiency of NCCIC. Among other activities, these recommendations called for the department to determine the applicability of the implementing principles and establish metrics and methods for evaluating performance; and address identified impediments. DHS agreed with the recommendations; however, as of April 2018, all nine recommendations remained unimplemented.

## Additional Actions by DHS Are Needed for Promoting and Assessing Private-Sector Adoption of the Cybersecurity Framework

An executive order issued by the President in February 2013 (E.O. 13636)[27] states that sector-specific agencies (SSA),[28] which include DHS, are to review the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (cybersecurity framework) [29] and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

[27] Exec. Order No. 13636, 78 Fed Reg. 11739, *Improving Critical Infrastructure Cybersecurity*, Vol.78, No. 33 (Feb. 19, 2013).

[28] Sector-specific agencies are federal agencies that are to serve as a federal interface for the prioritization and coordination of security and resilience efforts for the critical infrastructure sector for which they have lead roles. The sector-specific agencies are the Departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security, Transportation, and Treasury; the Environmental Protection Agency; and the General Services Administration.

[29] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014).

In February 2014, DHS launched the Critical Infrastructure Cyber Community Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage adoption of the framework across the critical infrastructure sectors.[30] In addition, DHS, as the SSA and co-SSA for 10 critical infrastructure sectors, had developed framework implementation guidance for some of the sectors it leads.

Nevertheless, we reported weaknesses in DHS's efforts to promote the use of the framework across the sectors and within the sectors it leads. Specifically, in December 2015, we reported that DHS did not measure the effectiveness of cyber community voluntary program to encourage use of the Cybersecurity Framework.[31] In addition, DHS and GSA, which are the co-SSAs for the government facilities sector, had yet to determine if sector implementation guidance should be developed for the government facilities sector. Further, in February 2018, we reported that none of the SSAs, to include DHS, had measured the cybersecurity framework's implementation by entities within their respective sectors, in accordance with the nation's plan for national critical infrastructure protection efforts.[32]

We made two recommendations to DHS to better facilitate adoption of the Cybersecurity Framework across the critical infrastructure sectors and within the government facilities sector. We also recommended that DHS develop methods for determining the level and type of framework adoption by entities across their respective sectors. DHS concurred with the two recommendations. As of April 2018, only the recommendation related to the government facilities sector has been implemented.

## DHS Needs to Better Measure Effectiveness of Cyber Risk Mitigation Activities with Critical Infrastructure Sector Partners

Presidential Policy Directive-21 issued by the President in February 2013, states that SSAs are to collaborate with critical infrastructure owners and

[30] Federal policy identifies 16 critical infrastructures: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[31] GAO, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, GAO-16-152 (Washington, D.C.: Dec. 2015).

[32] GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 2018).

operators to strengthen the security and resiliency of the nation's critical infrastructure.[33]

In November 2015, we reported that the SSAs, including DHS, generally used multiple public-private mechanisms to facilitate the sharing of cybersecurity related information.[34] For example, DHS used coordinating councils and working groups of federal and nonfederal stakeholders to facilitate coordination with each other. In addition, the department's NCCIC received and disseminated cyber-related information for public and private-sector partners.

Nevertheless, we identified deficiencies in critical infrastructure partners' efforts to collaborate to monitor progress towards improving cybersecurity within the sectors.[35] Specifically, the SSAs for 12 sectors, including DHS for 8 sectors, had not developed metrics to measure and report on the effectiveness of their cyber risk mitigation activities or their sectors' cybersecurity posture. This was because, among other reasons, the SSAs rely on their private-sector partners to voluntarily share information needed to measure efforts.

We made two recommendations to DHS—one recommendation based on its role as the SSA for 8 sectors and one recommendation based on its role as the co-SSA for 1 sector—to collaborate with sector partners to develop performance metrics and determine how to overcome challenges to reporting the results of their cyber risk mitigation activities.[36] DHS concurred with the two recommendations. As of April 2018, DHS has not demonstrated that it has implemented these recommendations.

## DHS has taken Steps to Identify its Workforce Gaps; However, It Urgently Needs to Take Actions to Identify Its Position and Critical Skill Requirements

In February 2018, we reported that DHS had taken actions to identify, categorize, and assign employment codes to its cybersecurity positions, as required by the Homeland Security Cybersecurity Workforce Assessment Act of 2014. However, its actions had not been timely and

[33] The White House, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 2013)

[34] GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress,* GAO-16-79 (Washington, D.C.: Nov. 19, 2015).

[35] GAO-16-79.

[36] GAO-16-79.

complete.[37] For example, DHS had not met statutorily defined deadlines for completing actions to identify and assign codes to cybersecurity positions or ensured that its procedures to identify, categorize, and code its cybersecurity positions addressed vacant positions, as required by the act. The department also had not (1) identified the individual within each DHS component agency who was responsible for leading and overseeing the identification and coding of the component's cybersecurity positions or (2) reviewed the components' procedures for consistency with departmental guidance.

In addition, DHS had not yet completed its efforts to identify all of the department's cybersecurity positions and accurately assign codes to all filled and vacant cybersecurity positions. In August 2017, DHS reported to the Congress that it had coded 95 percent of the department's identified cybersecurity positions. However, we determined that the department had, at that time, coded approximately 79 percent of the positions. DHS overstated the percentage of coded positions primarily because it excluded vacant positions, even though the act required the department to report such positions.

Further, although DHS had taken steps to identify its workforce capability gaps, it had not identified or reported to the Congress on its department-wide cybersecurity critical needs that align with specialty areas. The department also had not annually reported its cybersecurity critical needs to the Office of Personnel Management (OPM), as required; and it had not developed plans with clearly defined time frames for doing so.

We recommended that DHS take six actions, including ensuring that its cybersecurity workforce procedures identify position vacancies and responsibilities; reported workforce data are complete and accurate; and plans for reporting on critical needs are developed. DHS concurred with the six recommendations and stated that it plans to take actions to address them by June 2018.

In conclusion, DHS is unique among federal civilian agencies in that it is responsible for improving and promoting the cybersecurity of not only its own internal computer systems and networks but also those of other federal agencies and the private-sector owners and operators of critical infrastructure. Consistent with its statutory authorities and responsibilities

[37] GAO, *Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*, GAO-18-175 (Washington, D.C.: Feb. 6, 2018).

under federal policy, the department has acted to assist federal agencies and private-sector partners in bolstering their cybersecurity capabilities.

However, the effectiveness of DHS's activities has been limited or not clearly understood because of shortcomings with its programs and a lack of useful performance measures. DHS needs to enhance its capabilities; expedite delivery of services; continue to provide guidance and assistance to federal agencies and private-sector partners; and establish useful performance metrics to assess the effectiveness of its cybersecurity-related activities. In addition, developing and maintaining a qualified cybersecurity workforce needs to be a priority for the department. Until it fully and effectively performs its cybersecurity authorities and responsibilities, DHS's ability to improve and promote the cybersecurity of federal and private-sector networks will be limited.

Chairman Johnson, Ranking Member McCaskill, and Members of the Committee, this concludes my statement. I would be pleased to respond to your questions.

## GAO Contacts and Staff Acknowledgments

If you or your staffs have any questions about this testimony, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

GAO staff who made key contributions to this testimony are Larry Crosland, Tammi Kalugdan, David Plocher, Di'Mond Spencer, and Priscilla Smith.

# Related GAO Products

GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 15, 2018).

GAO, *Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*, GAO-18-175 (Washington, D.C.: Feb. 6, 2018).

GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, GAO-17-549 (Washington, D.C.: Sept. 28, 2017).

GAO, *Cybersecurity: Federal Efforts Are Under Way That May Address Workforce Challenges*, GAO-17-533T (Washington, D.C.: Apr. 4, 2017).

GAO, *Information Security: DHS Needs to Continue to Advance Initiatives to Protect Federal Systems*, GAO-17-518T (Washington, D.C.: Mar. 28, 2017).

GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

GAO, *Cybersecurity: Actions Needed to Strengthen U.S. Capabilities*, GAO-17-440T (Washington, D.C.: Feb. 14, 2017).

GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely*, GAO-17-163 (Washington, D.C.: Feb. 1, 2017).

GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016).

GAO, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, GAO-16-152 (Washington, D.C.: Dec. 17, 2015).

GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015).

# America, Democracy and Cyber Risk: Time to Act

**Prepared Statement**
**by**
**Honorable Eric Rosenbach**
**Co-Director of the Belfer Center for Science and International Affairs at Harvard Kennedy School; former Chief of Staff to the Secretary of Defense and Assistant Secretary of Defense for Homeland Defense and Global Security**

**Before the**

**United States Senate Committee on Homeland Security and Governmental Affairs**

**Hearing on**

**Mitigating America's Cybersecurity Risk**

**April 24, 2018**

---

Chairman Johnson, Ranking Member McCaskill, and distinguished members, thank you for calling today's hearing on mitigating America's cybersecurity risk and for the invitation to testify.

This is a time for action, and your Committee should play a key role. If American leaders in both the private sector and government continue to admire and debate our cyber vulnerabilities, the things that define the United States will steadily erode: democracy, a vibrant free-market economy, and the very values and freedoms that have guided our country since its foundation.

Here are some of the threats we've seen just this month: sophisticated ransomware shut down the city government of Atlanta for more than a week. Ransomware previously deployed by North Korean cyber operatives hit aircraft production lines at a major Boeing facility. DHS revealed that Russian cyber operatives have compromised major aspects of the internet's routing infrastructure. A recent White House report by the Council of Economic Advisers predicted that the cost of cybercrime to the US economy is set to top $100 billion annually.

The most concerning cyberattacks haven't yet cost the nation a dime, but could result in catastrophic consequences: DHS recently confirmed that Russian military intelligence operatives emplaced the malware used to take down the Ukrainian power grid (twice!) throughout energy infrastructure in the United States. And, as we approach the 2018 midterm elections, the risk of Russian cyber and information attacks against our election systems and campaigns is very real.

Against this backdrop, it is crucial that the nation comes together to build real capability and take real action to address these threats.

Russia is not the only potential threat. North Korea, Iran and China also maintain sophisticated offensive cyber capabilities. These countries also enjoy asymmetric advantages over the United States in cyberspace. Authoritarian societies often control their domestic media, censor online activity, and shield their citizens from outside information and cyber operations through national firewalls, such as the Great Firewall of China. Over the weekend, China's President Xi signaled that his government will increase its already tight control over internet and social media content as a national security priority, and Russia also has been intensifying its crackdown on internet and media freedoms in the past two years.

By contrast, the United States is a digital democracy. Our technological advances, high levels of digital connectivity, and transparent, open society make us vulnerable to foreign cyber and information attacks. In short, we live in a digital "glass house."

The cyber threat landscape we face is congested, and complex. Our adversaries are increasingly willing to attack non-government networks and private citizens, and to engage in widespread, indiscriminate attacks. North Korea's "WannaCry" cyberattack in 2017 affected organizations worldwide, including temporarily derailing operations at the UK's National Health Service. Russia's 2017 "NotPetya" cyberattack initially targeted Ukrainian organizations, but spread across the world, caused operations at major global transport and logistics companies to grind to a halt, and costing the private sector billions of dollars in damages.

As we look to the rest of 2018, the signals are clear: even organizations that are not targets of cyber attacks will be victims. From a CEO's perspective, the threat of collateral cyber damage is sobering—planning for and managing cyber risk has never been more complicated.

From the government's perspective, our adversaries' willingness to attack civilian targets makes the attack surface that we need to defend incredibly large. How should we prioritize resources and strategize for defense when the potential attack surface extends from government networks in D.C., to home routers in Wisconsin, hospital networks in Missouri and logistics hubs in Ohio, and everything in between?

This hearing and the Committee's framing of the problem we face—as one of *managing* cyber risk—are important. We will not eliminate cyber threats to America. To manage this cyber risk, the US Government must help lead a whole-of-nation effort to:

1. Bolster our domestic capabilities for defense and resilience;
2. Develop precise and legal offensive cyber capabilities to disrupt cyber and information attacks at their source; and
3. Adopt a clear, public deterrence posture.

**Bolster domestic defenses and resilience**

Cyber risk affects all corners of our economy and society. It is a whole-of-nation threat. It can only be successfully addressed with a whole-of-nation effort. The Government has a leading role to play. But ultimately, actions by private enterprise and non-government organizations will be key to our success.

Congress can do more to incentivize the private sector to act. In particular, Congress should:

- mandate that critical infrastructure providers adopt the NIST Cybersecurity Framework;
- establish baseline security standards for the manufacturers and distributors of "internet of things" devices, such as home routers, thermostats and security systems; and
- ensure that online platforms—including Facebook, Twitter, and YouTube—are not used as tools for foreign adversary information operations.

Bolstering private sector cyber defenses without regulation should be a priority. For example, one important lever to improve cyber risk management is a properly functioning market for cyber risk insurance. The government, and DHS and FBI in particular, can play a role in helping to unlock the promise of a mature cyber insurance market by improving collection and access to anonymized cyber incident data.

Significantly, DHS must empower the private sector to bolster its cyber defenses by continuing to strengthen information sharing with high-risk sectors. This is particularly urgent for election cybersecurity.

Organizations outside government must also play a role in protecting the nation from cyberattack. The Defending Digital Democracy Project, a bipartisan initiative I co-lead at Harvard's Belfer Center—along with Robby Mook and Matt Rhoades—works very closely with states to improve their ability to mitigate cyber risk. It's clear that the states take the cybersecurity of their systems very seriously. But states simply are not equipped to face the pointy-end of the spear of cyber attacks from state adversaries who are spending billions of dollars and dedicating thousands of cyber operators to advance their national interests.

Over the past nine months, our team of hard-working students, cyber security experts, technologists and political operatives:

- conducted field research at 34 state and local election offices;
- observed the November 2017 elections in three states;
- conducted a nationwide survey on cybersecurity with 37 states and territories; and
- engaged state and local election officials in three national "tabletop" simulations.

Our research and work found that under the leadership of Secretary Nielsen, Under Secretary Krebs and Assistant Secretary Manfra, DHS has improved information sharing with the states. We also saw that the Department's efforts to provide real capability are important: cybersecurity scans and risk assessments to the states have been productive and help mitigate risk. Congress should strongly support these efforts and provide DHS with the resources it needs to bring them to full maturity.

DHS has shown that bringing real capability to the table is essential. Congress should support the development of DHS' cybersecurity capability by providing the resources and authority for the Department to establish a robust, operationally-focused cybersecurity agency. This is more than bureaucratic box-shuffling: the nation needs an organization that provides critical infrastructure operators with the type of expert-level support that could make a real difference in mitigating the risk of foreign cyberattack.

And when it comes to protecting elections and critical infrastructure, state governments should look closely at strengthening the role that the National Guard and state-run fusion centers play in election-related threat information sharing. This potent combination will provide an important hub for sharing threat intelligence and cybersecurity capability.

**Develop precise and legal offensive cyber capabilities**

Even with improved cyber defenses, we will of course not be immune from attack. To complement the work that DHS does, the US Government, led by the Department of Defense, must bolster real capabilities to disrupt and degrade cyber and information operations at their source. In particular, there is a need to:

- **Strengthen indications and warning of cyber and information attacks.** The Intelligence Community, and the National Security Agency in particular, need to bolster the "early warning" system for information operations which target US democratic institutions.
- **Bolster Cyber Command's capability to address information operations.** The US military lacks the structure and capability necessary to defend the nation from future attacks. Special Operations Command has historically led Department of Defense efforts in information operations, but the lead must now shift to Cyber Command in order to strengthen the nexus of cyber and information operations capabilities necessary for the information age. That said, the Department of Defense's recent efforts to combat ISIS through a joint SOCOM-CYBERCOM effort, known as Task Force Ares, represents an outstanding model for future operations.
- **Take a leading role in building international capacity to disrupt the proliferation of black-market destructive malware.** The Proliferation Security Initiative for weapons of mass destruction—supported by over 100 countries—provides an analogous model for action.
- **Take a more active role in disrupting and dismantling botnets used by criminals and foreign adversaries.** Law enforcement organizations, led by the FBI and Department of Justice, alongside the Department of Defense when needed, should work very closely with telecommunications companies and international partners to neutralize botnets.

**Adopt a clear, public deterrence posture**

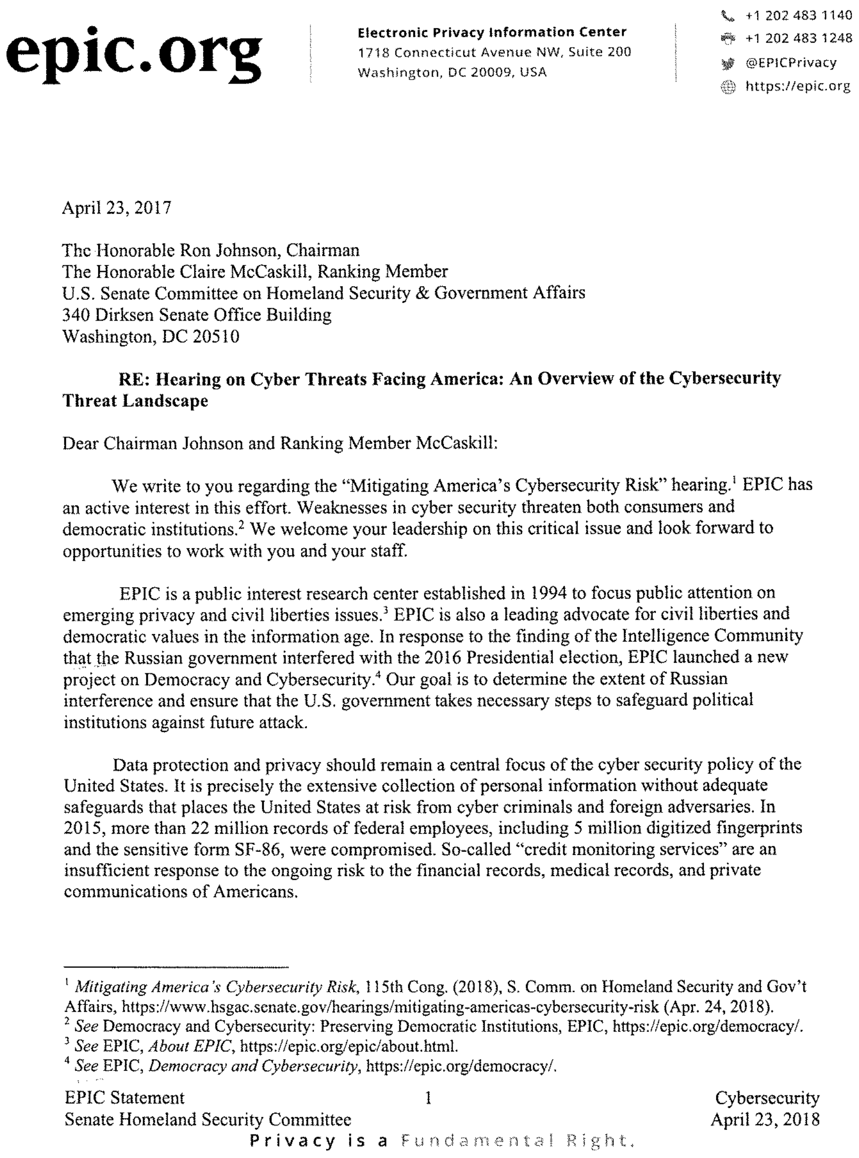
Our national response to cyber and information attacks—both against the United States and our allies—has been consistently weak.

Imagine if we found out during the Cold War that Soviet operatives had placed secret explosives in parts of the electric grid all around the United States. Would US leaders have stood by and debated the nature of the threat, or would they have acted?

The United States must urgently act to bolster its cyber deterrence posture by both raising the costs of attacks and decreasing the benefits to hostile actors of engaging in cyber and information operations. Recently, the increased willingness of the Intelligence Community, DHS and FBI to publicly attribute attacks to foreign is crucial and a positive first step. This must happen more often, and more swiftly, and be accompanied by consequences. The recent move by the current administration to increase sanctions on Russian entities involved in cyber attacks against Ukraine and the United States is another step in the right direction, but again not nearly enough.

We also need to more consistently respond to cyberattacks against our allies and partners. Russia frequently uses Ukraine and other of its neighbors as "testing grounds" for its offensive information and cyber operations. However, Las Vegas rules do not apply in the digital age. If we permit Russia to test and perfect these tools on another country, they will eventually be used against us. Additionally, as the NotPetya cyberattack I spoke about earlier demonstrates, even attacks that are intended to only affect entities in one country can enter the global supply chain and quickly spread to damage US actors and interests.

In sum, defending our nation from state adversaries is ultimately a government responsibility. But we will never be able to deter or defend ourselves against all cyberattacks. The United States became the world's technological leader by harnessing the talents of thousands of public and private sector innovators. To protect our technological edge, and our nation, we must once again mobilize all parts of society in a whole-of-nation effort.



epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

April 23, 2017

Thc Honorable Ron Johnson, Chairman
The Honorable Claire McCaskill, Ranking Member
U.S. Senate Committee on Homeland Security & Government Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

**RE: Hearing on Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape**

Dear Chairman Johnson and Ranking Member McCaskill:

We write to you regarding the "Mitigating America's Cybersecurity Risk" hearing.[1] EPIC has an active interest in this effort. Weaknesses in cyber security threaten both consumers and democratic institutions.[2] We welcome your leadership on this critical issue and look forward to opportunities to work with you and your staff.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[3] EPIC is also a leading advocate for civil liberties and democratic values in the information age. In response to the finding of the Intelligence Community that the Russian government interfered with the 2016 Presidential election, EPIC launched a new project on Democracy and Cybersecurity.[4] Our goal is to determine the extent of Russian interference and ensure that the U.S. government takes necessary steps to safeguard political institutions against future attack.

Data protection and privacy should remain a central focus of the cyber security policy of the United States. It is precisely the extensive collection of personal information without adequate safeguards that places the United States at risk from cyber criminals and foreign adversaries. In 2015, more than 22 million records of federal employees, including 5 million digitized fingerprints and the sensitive form SF-86, were compromised. So-called "credit monitoring services" are an insufficient response to the ongoing risk to the financial records, medical records, and private communications of Americans.

[1] *Mitigating America's Cybersecurity Risk*, 115th Cong. (2018), S. Comm. on Homeland Security and Gov't Affairs, https://www.hsgac.senate.gov/hearings/mitigating-americas-cybersecurity-risk (Apr. 24, 2018).
[2] *See* Democracy and Cybersecurity: Preserving Democratic Institutions, EPIC, https://epic.org/democracy/.
[3] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[4] *See* EPIC, *Democracy and Cybersecurity*, https://epic.org/democracy/.

Strong encryption policy and robust technical measures must be enacted to safeguard personal data. Weaknesses in security standards create vulnerabilities for American businesses and consumers that will be exploited by foreign adversaries. Where it is possible to minimize or eliminate the collection of personally identifiable information, the risk to the American public will be reduced. Strong encryption keeps the information of the American people secure, which by extension makes the nation secure. And perhaps it is a firewall and not a border wall that the United States needs to safeguard its national interests at this moment in time.[5]

The Cyber Security Information "Sharing" Act is now in force. That law facilitates the transfer of customer and client data from the private sector to the government, raising widespread concerns among technical experts and privacy organizations about the protection of personal information. While we favor a cooperative relationship between companies and the federal government concerning cyber security, the federal government must respect the privacy obligations of private companies and ensure the transparency of its own conduct. In the cyber security domain, as with other programs supported by taxpayer dollars, the government must uphold the law and remain open and accountable.

Finally, *Congress should strengthen the federal Privacy Act*. Personal data stored in federal agencies remains one of the key targets of criminal hackers and foreign adversaries. Significant steps were taken by the last administration to establish a Federal Privacy Council and to coordinate privacy protection across the federal agencies. Still, more should be done, including updates to the federal privacy law and the establishment of a data protection agency in the United States.

The United States should stand for the protection of democratic institutions, the rule of law, an independent judiciary and the protection of fundamental rights. Our national security strategy should reflect these values.

We ask that this Statement be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

/s/ Christine Bannan
Christine Bannan
EPIC Policy Fellow

[5] Garry Kasparov (@kasparov63), "If the US is serious about stopping a real danger from abroad, it should build a better firewall, not a bigger border wall." (12:34 PM - 22 Jan 2018), https://twitter.com/Kasparov63/status/955539139121819649.

**Post-Hearing Questions for the Record**
**Submitted to Assistant Secretary Jeanette Manfra**
**From Senator Claire McCaskill**

**"Mitigating America's Cybersecurity Risk"**

**April 24, 2018**

| | |
|---|---|
| **Question#:** | 1 |
| **Topic:** | Binding Operational Directive |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Claire McCaskill |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** In October, DHS issued Binding Operational Directive (BOD) 18-01 to enhance email and web security by making it more difficult for a bad actor to mimic legitimate email communications from federal agencies.

How many and which federal agencies have complied with the BOD? How many and which agencies are overdue?

What is DHS's plan for promoting compliance with this BOD for the remaining agencies?

**Response:** On October 16, 2017, the Department of Homeland Security (DHS) issued Binding Operational Directive (BOD) 18-01, Enhance Email and Web Security. The BOD is a compulsory direction to federal agencies to implement specific email and web security standards that have been widely adopted in industry. The security practices ensure the integrity and confidentiality of Internet-delivered data, minimize spam, and better protect users who might otherwise fall victim to a phishing email that appears to come from a government-owned system.

Regarding the email security requirements, 69% of agencies were over 80% compliant as of July 24, 2018. Regarding web security requirements, 45% of agencies were over 80% compliant as of July 24, 2018, across all web tasks.

Agencies are working diligently to comply with this BOD. According to monthly reports provided to DHS, agencies have articulated challenges with vendors, a lack of internal expertise to implement email and web security standards, risk to mission and business operations, insufficient funding, and concerns around DMARC implementation. A large number of agencies have cited funding and resource challenges to implementation. DHS is working with the Office of Management and Budget to address the concerns.

| | |
|---|---|
| **Question#:** | 1 |
| **Topic:** | Binding Operational Directive |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Claire McCaskill |
| **Committee:** | HOMELAND SECURITY (SENATE) |

DHS continues to remain actively engaged in extensive outreach to the agencies to encourage rapid implementation of outstanding BOD 18-01 requirements. In addition to a large number of calls and emails with agencies, DHS has hosted technical discussion to address agency questions and concerns. Through these discussions, DHS works with agencies to address common challenges and advance implementation across the government.

| | |
|---|---|
| **Question#:** | 2 |
| **Topic:** | Tools and Authorities |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Claire McCaskill |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** It is discouraging that the federal government repeatedly fails to implement basic cybersecurity standards, even when directed to by both OMB and DHS. What additional tools or resources does DHS need to ensure better compliance across the .gov space?

Does DHS need any more, enhanced, or different authorities to better assist the federal government with addressing its cybersecurity vulnerabilities?

**Response:** Consistent with the Federal Information Security Modernization Act of 2014, the National Cybersecurity Protection Act of 2014, and the Cybersecurity Act of 2015, among other laws and policies that have been implemented, DHS has broad authorities to assist federal agencies with mitigation of their cybersecurity risk. Additionally, DHS has authority to issue compulsory directives to federal agencies. While progress is most certainly still needed, these authorities have enabled repeated successes as federal agencies improve their cybersecurity risk management posture. Fully funding the President's budget request is critical to enabling DHS and federal agencies to implement key cybersecurity priorities.

One example of how these authorities have been leveraged to implement repeated successes is through binding operational directives (BODs). Overall, DHS is satisfied with the current compliance rate across existing BODs and is pleased with the significant impact these directives have had on Federal cybersecurity. For example, BOD 15-01 reduced the number of outstanding critical vulnerabilities to Internet-facing systems across the federal government by over 99 percent. It also altered the way Federal agencies review and respond to DHS's Cyber Hygiene scans. As another example, BOD 16-01 and 16-02 have been instrumental in identifying and addressing long-standing constraints related to risks including widespread use of legacy information technology (IT). DHS has leveraged enhanced visibility into agency challenges to advocate for security changes and collaborated with OMB on funding decisions required to resolve these persistent problems. Across all BODs, DHS has observed department-level offices coordinate across their sub-components to implement BOD requirements.

Current BOD authorities are an important DHS tool used to drive significant cybersecurity change, impact cross-government performance, and mitigate substantial cyber threats and risks to Federal information systems. DHS has found that the key to successful BOD implementation is persistent interaction and support to individual agency teams. This includes weekly discussions on BOD actions, associated constraints, and technical guidance to ensure agencies are informed and on track with the implementation

| | |
|---|---|
| **Question#:** | 2 |
| **Topic:** | Tools and Authorities |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Claire McCaskill |
| **Committee:** | HOMELAND SECURITY (SENATE) |

of these critical actions. DHS has found these directives to be an effective means by which DHS can coordinate government-wide actions, implement critical requirements, raise awareness, and emphasize the urgency of specific actions across all levels of Federal leadership.

**Post-Hearing Questions for the Record**
**Submitted to Assistant Secretary Jeanette Manfra**
**From Senator Heidi Heitkamp**

**"Mitigating America's Cybersecurity Risk"**

**April 24, 2018**

| | |
|---|---|
| **Question#:** | 3 |
| **Topic:** | STOP THINK CONNECT Campaign |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Heidi Heitkamp |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** One of my priorities in Congress has been to identify opportunities to leverage and promote good cyber-hygiene practices. Cyberattacks rely on vulnerabilities to exploit and infiltrate systems and networks, and these vulnerabilities are created and compounded when people use bad cyber practices. Systems are only as secure as the weakest link, and that is why it is so essential that we make sure individuals practice good cyber hygiene.

I appreciate that you mentioned the partnership between DHS and the National Cyber Security Alliance (NCSA) to educate the public on the importance of adopting good cyber-hygiene practices. In your view, how effective has this partnership, particularly as it relates to the STOP. THINK. CONNECT. campaign, been in educating the public on cyber-hygiene?

Are there aspects of the program that you believe could be enhanced? Is there a role Congress should play in supporting the efforts of DHS or the NCSA?

**Response:** The STOP. THINK. CONNECT. Campaign was launched in 2010 as a national cybersecurity public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safe and more secure online. The Department of Homeland Security (DHS) leads the federal government's engagement with the campaign that includes the National Cyber Security Alliance and a coalition of private companies, non-profits, and government organizations. The STOP. THINK. CONNECT. campaign has been an effective tool for elevating the nation's awareness of cybersecurity and its association with national security and the safety of our personal lives; engaging the American public, the private sector, and state and local governments in our nation's effort to improve cybersecurity; and communicating approaches and strategies for the public to keep themselves, their families, and their communities safer online. Congress plays an important role by continuing to support

| | |
|---|---|
| **Question#:** | 3 |
| **Topic:** | STOP THINK CONNECT Campaign |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Heidi Heitkamp |
| **Committee:** | HOMELAND SECURITY (SENATE) |

funding for cybersecurity outreach and awareness activities, including the National Cybersecurity Awareness campaign.

| | |
|---|---|
| **Question#:** | 4 |
| **Topic:** | Further Cyber-Hygiene Education |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Heidi Heitkamp |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** In addition to the partnership between DHS and the NCSA, are there other groups or organizations that DHS has engaged or is in partnership with to educate the public on cyber-hygiene? To what extent is there a DHS strategy to partner with various groups and organizations to educate the public on cyber-hygiene?

**Response:** The partnership between the Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA) is the primary way DHS engages in direct public awareness campaigns to educate the public on cyber-hygiene. In addition to this partnership, DHS regularly publishes information regarding basic cyber hygiene on its website (https://www.us-cert.gov/) and by leveraging social media. This information is also pushed to a broad range of stakeholders who are able to leverage it for further public awareness efforts.

| | |
|---|---|
| **Question#:** | 5 |
| **Topic:** | Small Businesses |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Heidi Heitkamp |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** As you know, small businesses can be particularly susceptible to cyber-attacks because they may not have the resources or training they need to protect themselves. Nevertheless, basic cyber hygiene can have a meaningful impact on their security posture. I understand that DHS provides resources, such as voluntary assessments and the Toolkit for Small and Midsize Businesses, to help businesses strengthen their cybersecurity.

To what extent are businesses using these resources?

Unfortunately, a number of small businesses are not taking pro-active steps to protect against cyber threats. Convincing businesses that they are legitimate targets for cyber-attacks is absolutely essential to motivating them take cybersecurity seriously.

In your view, how should the federal government go about persuading small businesses, especially those who have not yet been impacted by cybercrime, to take cybersecurity seriously?

**Response:** It is important to recognize that small businesses include a highly diverse set of entities that range in cybersecurity risk management maturity from very unsophisticated to highly sophisticated. The Department of Homeland Security (DHS) has a range of capabilities and information that are ideal for cybersecurity consumers at varying levels of maturity. In other words, some of the more advanced cybersecurity capabilities or technical alerts are not ideal for a consumer with very little technical expertise. However, cybersecurity service providers are engaged with DHS and leverage such information to enhance services that they may provide to small businesses. DHS and our federal partners, such as the Small Business Administration, the Federal Trade Commission, and the National Institute of Standards and Technology, will continue to conduct outreach and engage in public awareness campaigns that play a role in persuading small businesses to take cybersecurity seriously.

| | |
|---|---|
| **Question#:** | 6 |
| **Topic:** | Recruiting and Retention |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Heidi Heitkamp |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Recruiting and retaining a robust cybersecurity workforce remains a consistent challenge for the federal government. However, I am enthusiastic that DHS is in the process of implementing a new 21st century personnel system that will allow the agency to hire personnel quickly and offer competitive salaries.

Could you discuss DHS' efforts to implement this system and the impact the system, once implemented, will have on the National Cybersecurity and Communications Integration Center?

**Response:** DHS thank Congress for the authority granted to the Department in Section 3 of the Border Patrol Agent Pay Reform Act of 2014 to address recruitment and retention of our nation's top cybersecurity professionals to help DHS accomplish its mission. DHS continues to manage a variety of activities to prepare for the launch of the new cybersecurity-focused personnel system. As the Secretary works to prescribe the required regulation, in coordination with the Office of Management and Budget and the Director of the Office of Personnel Management, the Office of the Chief Human Capital Officer (OCHCO) is finalizing the design of the system, preparing new policies and business processes, and planning for a smooth implementation with DHS Components and across the Federal enterprise. Some key focus areas for the remainder of FY 2018 include:

- Hiring key federal staff and specialized contractor support to oversee and operate the new personnel system, which is expected to be more data and mission driven;
- Completing additional cybersecurity labor market research, including consulting with the Department of Defense (DOD) and the Office of the Director of National Intelligence, Chief Human Capital Office, to establish pay structures and flexibilities for their initial use;
- Conducting an industrial/organizational psychology study of new standards for describing cybersecurity work to ensure the legal defensibility of upcoming hiring and pay decisions;
- Developing and validating the suite of assessment tools that will be used to screen candidates and ensure that the individuals hired under the new system can truly execute complex, technical cybersecurity work;
- Transforming existing cross-Component cybersecurity workforce coordinating councils to execute and review upcoming hiring, pay, and other human capital actions that will require cybersecurity subject matter expert input; and

| | |
|---|---|
| **Question#:** | 6 |
| **Topic:** | Recruiting and Retention |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Heidi Heitkamp |
| **Committee:** | HOMELAND SECURITY (SENATE) |

- Analyzing the cybersecurity work across Components and isolating the priority organizations and functions that will participate in the initial phase of hiring under the new system.

DHS has already identified hiring for the National Cybersecurity and Communications Integration Center (NCCIC) as an implementation priority, and expects the new personnel system to enhance NCCIC operations in a variety of ways. For example, the new personnel system is designed to ensure:

- A steady pipeline of available and carefully-screened talent for the specialized work of the NCCIC; and
- New methods for tailoring assignments, career development, and compensation to better recognize top talent and ensure employees' skills keep pace with the field and the NCCIC mission.

DHS believes such human capital changes will enable the NCCIC to:

- Attract higher quality talent;
- Retain top talent longer;
- Manage top talent more effectively;
- Modernize and improve the employee experience; and
- Deploy surge expertise—including that assigned to other DHS Components—more quickly around incidents and new threats.

**Question:** Is there a timeline on when you expect the new personnel system to go live?

**Response:** DHS is committed to making our new cybersecurity service personnel system operational as quickly as possible, and the implementation effort is gaining momentum. Currently, DHS is targeting late 2019 for phase 1 launch of the system, to include hiring of an initial cadre of cybersecurity experts. As we reach notable milestones, DHS intends to keep the Committee informed of progress and timelines.

| | |
|---|---|
| **Question#:** | 7 |
| **Topic:** | 2018 Elections |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Heidi Heitkamp |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** In your testimony, you discuss DHS's work with states in preparation for this year's state and federal elections. What I am interested to know - what is the capacity of DHS to handle a sizeable and diverse attack?

What type of rapid response program and deployment system do you have in place for the 2018 elections to address a myriad of challenges all happening close to the election and relatively close in proximity or simultaneously? If you have a program and system in place, is it capable of handling widespread, multi-state attacks? Do you have the resources you need for this - if not what more do you need?

You have taken steps to evaluate state cybersecurity efforts in response to lessons learned from and since the 2016 elections.

Do you believe broadly that states have taken the necessary steps to prevent and respond to cyberattacks during the course of the 2018 election? If not, do you believe that most states will have taken these steps prior to election day in November?

Broadly speaking, what are the largest gaps that still exist in state-level electoral cybersecurity? How do states collaborate better with the DHS and the federal government to close these gaps? In a best case scenario, how long would it take to close the most glaring gaps prior to the elections in November?

**Response:** During cyber incidents, the Federal Government's roles and responsibilities are guided by statutory authority, Presidential Policy Directive 41, and the National Cyber Incident Response Plan. During cyber incidents, federal agencies undertake three concurrent lines of effort: threat response, asset response, and intelligence support and related activities. During significant incidents, the Department of Justice (DOJ), acting through the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force, is the federal lead agency for threat response activities; the Department of Homeland Security (DHS), acting through the National Cybersecurity and Communications Integration Center, is the federal lead agency for asset response activities; and the Office of the Director of National Intelligence (ODNI), through the Cyber Threat Intelligence Integration Center, is the federal lead agency for intelligence support and related activities. Sector-Specific Agencies for affected critical infrastructure sectors contribute to the interagency response effort by leveraging their well-established relationships within their sector and understanding the potential business or operational impacts on private sector critical infrastructure. During a widespread, multi-state cyber incident, DOJ, DHS, and ODNI coordinate the full resources of the federal government,

| | |
|---|---|
| **Question#:** | 7 |
| **Topic:** | 2018 Elections |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Heidi Heitkamp |
| **Committee:** | HOMELAND SECURITY (SENATE) |

state and local governments, and private sector expertise in response. DHS has elections-related points of contact in all 50 states, enabling quick engagement with election officials when necessary. Additionally, DHS, through the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), has established a real-time information sharing portal for election officials to use on Election Day.

DHS appreciates Congresses continued support to provide necessary resources to carry out this mission. In addition to funding provided to DHS, the Consolidated Appropriations Act, 2018, provided $380 million to the Election Assistance Commission (EAC) to make payments to states for activities to improve the administration of elections, including to enhance election technology and make election security improvements. These funds were designed to close gaps and enhance the cybersecurity of election infrastructure, and the Joint Explanatory Statement accompanying the Act provided additional guidance regarding expenditure of these funds. DHS and the EAC have worked through the Election Infrastructure Subsector's Government Coordinating Council to collaborate with the sector on funding guidance for the election community. This guidance provides direction to the election community regarding possible considerations for the use of newly available election funding, as well as support for procurement decisions regarding use of the funding. Additionally, DHS provides local and regional support through Cybersecurity Advisors and Protective Security Advisors, all of whom are available to assist election officials in discussing their unique implementation challenges and security concerns.

Under our system of laws, federal elections are administered by state and local election officials in thousands of jurisdictions across the country. These officials manage election infrastructure and ensure its security and resilience on a day-to-day basis. DHS and our federal partners have formalized the prioritization of voluntary cybersecurity assistance for election infrastructure similar to that which is provided to a range of other critical infrastructure entities, such as financial institutions and electric utilities.

DHS regularly coordinates with the intelligence community and law enforcement partners. Since 2016, DHS has convened federal government and election officials regularly to share cybersecurity risk information and to provide assistance. The Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) is making progress on strategic security initiatives for the sector. DHS has worked with the GCC to establish the EI-ISAC. With over 600 members the EI-ISAC serves as a sector-specific hub of information sharing with and among the elections sector.

DHS and election officials have made tremendous strides. DHS is committed to working collaboratively with those on the front lines of administering our elections to secure

| | |
|---|---|
| **Question#:** | 7 |
| **Topic:** | 2018 Elections |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Heidi Heitkamp |
| **Committee:** | HOMELAND SECURITY (SENATE) |

election infrastructure from risks. The establishment of government and sector coordinating councils are building the foundations for this enduring partnership not only in 2018, but for future elections as well. We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. However, we recognize that there is a significant technology deficit across state and local governments, and State and local election systems, in particular. It will take significant and continual investment to ensure that election systems across the nation are upgraded and secure, with vulnerable systems retired.

| | |
|---|---|
| **Question#:** | 8 |
| **Topic:** | Cyberattacks on Energy Infrastructure |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Heidi Heitkamp |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** I am deeply concerned about cyberattacks on our nations electrical grid and facilities - and more broadly our energy infrastructure, including pipelines, drilling rigs, and numerous other components and tools of our vast energy industry. Russia has already attacked the energy systems in Ukraine - and we know that several state actors have been discovered rooting around in the systems of various U.S. utilities, facilities, and energy infrastructure.

Where would you say these systems and facilities rank in terms of priorities for foreign state actors? Are the companies and owners of these targeted facilities treating the threat appropriately to match this prioritization by foreign state actors?

What are your biggest concerns related to cyberattacks on these systems and infrastructure? Are we doing enough at the federal and state government level to address these challenges?

What more can the federal government do to assist utilities, facility owners, and energy infrastructure in preparing for, responding to, and sharing information about cyberattacks?

**Response:** The Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD), in coordination with Sector-Specific Agencies (Departments of Energy (DOE) and Transportation, and DHS's Transportation Security Administration (TSA), work closely with entities in the energy and transportation sectors to enhance the security and resiliency of our electric grid and related facilities. As part of the President's Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, DHS and the DOE partnered with other federal agencies and electricity industry stakeholders to conduct an assessment of the potential scope and duration of a prolonged power outage associated with a significant cyber incident, as well as an evaluation of the readiness and gaps in the United States' ability to manage and mitigate consequences of a cyber incident against the electric subsector. This assessment concluded that the U.S. is, in general, well prepared to manage most electricity disruptions, though there are particular areas where catastrophic considerations and emerging threats reveal capability gaps against cyberattacks.

To address these gaps, the assessment outlines areas spanning from improving public communications across officials at all levels, expanding cybersecurity technical expertise and information sharing, and integrating and augmenting planning and analytic capabilities for long term disruption and potential consequences and impacts resulting

| | |
|---|---|
| **Question#:** | 8 |
| **Topic:** | Cyberattacks on Energy Infrastructure |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Heidi Heitkamp |
| **Committee:** | HOMELAND SECURITY (SENATE) |

from such a disruption. In addition, early integration of cybersecurity into system design; funding for cybersecurity investments, particularly for smaller utilities; and strong workforce development would holistically support national preparedness of the Nation's electric infrastructure. The report can be found online at: https://www.energy.gov/downloads/report-strengthening-cybersecurity-federal-networks-and-critical-infrastructure.

| | |
|---|---|
| **Question#:** | 9 |
| **Topic:** | Tribes and Tribal Nations |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Heidi Heitkamp |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** I noticed throughout your testimony mentions of working with or making programs and assistance available to tribes and tribal nations. As you probably know, much of Indian Country is incredibly rural, remote, and isolated - leaving them vulnerable even when everything is working fine - but a cyberattack in or around Indian Country could have devastating impacts because of these very surroundings.

What level of participation or collaboration has there been between DHS and tribes and tribal nations on cybersecurity issues?

What type of outreach program does DHS have in place to make tribes and tribal nations aware of potential threats, available federal programs and assistance - and what consultation protocols does DHS have in place to work with tribal governments in setting up cybersecurity protocols and partnerships?

Has DHS ever evaluated broadly the potential threats and the resources and personnel available to meet these threats in Indian Country? If no, why not? If yes, what did you find?

**Response:** The Department of Homeland Security (DHS) is authorized to provide cybersecurity assistance to federal and non-federal entities. Tribes and tribal nations are included in DHS's engagement with state, local, tribal, and territorial governments. While the level of participation and collaboration between DHS, and tribes and tribal nations on cybersecurity issues could be more robust, DHS shares information and makes available a range of capabilities that are available to all stakeholders. Additionally, tribes and tribal nations can join the Multi-State Information Sharing and Analysis Center (MS-ISAC), an organization funded by DHS. MS-ISAC includes membership of state, local, tribal, and territorial governments, enabling members to share cybersecurity information and collaborate with each other. Also, through DHS's Office of Intergovernmental Affairs, DHS engages with tribes and tribal nations across the range of homeland security missions.

**Post-Hearing Questions for the Record**
**Submitted to Assistant Secretary Jeanette Manfra**
**From Senator Rand Paul**

**"Mitigating America's Cybersecurity Risk"**

**April 24, 2018**

| | |
|---|---|
| **Question#:** | 10 |
| **Topic:** | National Security Threat |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Nearly all Americans protect their private and commercial communications with encryption tools like Virtual Private Networks (VPN) and Transport Layer Security (TLS). A number of governments have deliberately compromised the integrity of popular encryption tools. Of course, a flaw designed to make encryption more tractable by one government may be exploited by another.

Do flaws impacting the confidentiality of popular encryption tools represent a national security threat?

**Response:** Encrypting data is an important way to protect sensitive information by ensuring that data can only be read by the person who is authorized to have access to it. When vulnerabilities in encryption tools are discovered, the ability to protect sensitive information may be jeopardized. If these vulnerabilities are not mitigated, it could represent a national security threat if the tools are being used to protect information that is critical to our national security.

At the same time, we must find a way to balance the need to secure data with the need for the homeland security enterprise to access data in order to safeguard the public, investigate crimes, and prevent future criminal activity, including significant homeland security threats like terrorism.

| | |
|---|---|
| **Question#:** | 11 |
| **Topic:** | Secure by Default |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** "Cyber hygiene" is at the core of NPPD's Binding Operational Directives. Cybersecurity experts recommend service providers improve cyber hygiene by ensuring their products are "secure by default," meaning encryption and other security features are enabled without the user needing to opt-in.

Would you recommend that companies ensure cell phones, messaging applications, and other services Americans rely on be "secure by default"?

**Response:** Strengthening the security and reliability of the cyber ecosystem is a key cybersecurity goal of the Department of Homeland Security's (DHS's) risk management approach. Such efforts help shift the advantage away from malicious cyber actors toward those protecting cyberspace. Without recommending specific practices included in the much broader definition of "secure by default," DHS believes that security should be built into devices by default. While there are exceptions, in too many cases economic drivers or lack of awareness of the risks cause businesses to push devices to market with little regard for their security. Building security in at the design, development, and production phases reduces potential disruptions and avoids the much more difficult and expensive endeavor of attempting to add security to products after they have been developed and deployed. Encryption is one security feature that strengthens the protection and confidentiality of information.

| | |
|---|---|
| **Question#:** | 12 |
| **Topic:** | Key Escrow Systems |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Some government officials seek to weaken the confidentiality of popular cryptography systems. These so-called "responsible encryption" proposals are variations of key escrow systems, where affected encrypted channels would be accessible by third parties.

Are key escrow systems appropriate for widespread use by the federal government?

Would compromise of a key escrow system used to access American cell phones, private messages, or other widespread technology represent a national security threat?

**Response:** Encryption provides an effective means to secure data but can undermine public safety efforts by impeding lawful access to the content of communications during investigations into serious crimes, including terrorism. The increased use of encryption is driven, in part, by market demand and concerns over cybersecurity, privacy, and human rights. We must find a way to balance the need to secure data with the need for the homeland security enterprise to access data in order to safeguard the public, investigate crimes, and prevent future criminal activity, including significant homeland security threats like terrorism.

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Mr. Rosenbach indicated reporting requirements may impress an excessive burden on DHS and the Government Accountability Office (GAO).

Please provide for the record a list of internal reports DHS has been charged to complete. Include all reports delivered over the last three years, reports not yet completed, and recurring reports to be delivered in the future.

**Response:**

**FY 2015, 2016, and 2017 DHS Congressional Appropriations Reports**

| Component/ Office | Appropriations Reports Required by Congress | Statutorily Recurring | Fiscal Year Required |
|---|---|---|---|
| CBP | 5-Year Construction Plan for Federal Land Ports of Entry | Yes | 2016 |
| CBP | 5-Year Construction Plan for Federal Land Ports of Entry | | 2017 |
| CBP | AD/CVD Actions and Compliance Initiatives | Yes | 2016 |
| CBP | AD/CVD Collection of Outstanding Claims | | 2015 |
| CBP | AD/CVD Collection of Outstanding Claims | | 2016 |
| CBP | AD/CVD Collection of Outstanding Claims | | 2017 |
| CBP | AD/CVD Enforcement Actions and Compliance Initiatives | Yes | 2017 |

| | |
|---|---|
| **Question#:** | 3 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| CBP | AD/CVD Liquidation Instructions | | 2016 |

| Component/ Office | Appropriations Reports Required by Congress | Statutorily Recurring | Fiscal Year Required |
|---|---|---|---|
| CBP | AD/CVD Liquidation Instructions | | 2017 |
| CBP | AD/CVD New Shipper Single-Entry Bonds | | 2015 |
| CBP | AD/CVD New Shipper Single-Entry Bonds | | 2016 |
| CBP | AD/CVD New Shipper Single-Entry Bonds | | 2017 |
| CBP | Automated Commercial Environment Semiannual Report - First and Second Quarters FY 2016 | | 2016 |
| CBP | Automated Commercial Environment Semiannual Report - Third and Fourth Quarters FY 2016 | | 2016 |
| CBP | Biometric Exit & H1-B and L-1 Fees Spend Plan | | 2017 |
| CBP | Border Patrol Agent Pay Reform | | 2016 |
| CBP | Border Security Fencing, Infrastructure, and Technology Multi-Year Investment and Management Plan (FY 2015 – FY 2018) | | 2015 |
| CBP | Border Security Improvement Plan | | 2017 |
| CBP | CBP Body-Worn Camera Feasibility Study and Camera Technology Report | | 2015 |
| CBP | CBP FY 2015 Financial Plan | | 2015 |
| CBP | CBP Obligation and Hiring Plan - Q1 | | 2016 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| CBP | CBP Obligation and Hiring Plan - Q2 | | 2016 |

| Component/ Office | Appropriations Reports Required by Congress | Statutorily Recurring | Fiscal Year Required |
|---|---|---|---|
| CBP | CBP Obligation and Hiring Plan - Q3 | | 2016 |
| CBP | CBP Obligation and Hiring Plan - Q4 | | 2016 |
| CBP | CBP Officer Overtime | | 2017 |
| CBP | CBP Staff Professionalism | | 2015 |
| CBP | Compliance with National Standards on Transport, Escort, Detention, and Search (TEDS) | | 2017 |
| CBP | Comprehensive Biometric Entry and Exit Data System Implementation | | 2016 |
| CBP | Comprehensive Biometric Entry/Exit Plan | | 2015 |
| CBP | Current Preclearance Operations | | 2015 |
| CBP | Current Shrimp Import Regime Plan | | 2016 |
| CBP | Distribution of Interest to Affected Domestic Producers Under the CDSOA | | 2015 |
| CBP | Drawback Claims for Refund of Certain Excise Taxes | | 2017 |
| CBP | Entry/Exit Overstay Report | Yes | 2016 |
| CBP | Entry/Exit Overstay Report, Fiscal Year 2016 | Yes | 2017 |
| CBP | Expedited Hiring Plan | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| Component/ Office | Appropriations Reports Required by Congress | Statutorily Recurring | Fiscal Year Required |
|---|---|---|---|
| CBP | FY 2015 – FY 2018 Multi-Year Investment and Management Plan for Information and Technology | | 2015 |
| CBP | Illegal Trafficking of Wildlife and Other Natural Resources | | 2015 |
| CBP | Inspection and Detection Technology Multi-Year Investment and Management Plan (FY 2015–FY 2018) | | 2015 |
| CBP | Inspection and Detection Technology Multiyear Investment Plan | | 2017 |
| CBP | Intelligence Capability Assessment Results | | 2017 |
| CBP | Inventory of Single Transaction Bonds | | 2017 |
| CBP | Investigation into Deaths in Custody and Use-of-Force Incidents | | 2016 |
| CBP | Investigations into Deaths in Custody and Use-of-Force Incidents | | 2015 |
| CBP | Land Border Wait Times (Automated Wait Time and Trade Facilitation Performance Measures) | | 2016 |
| CBP | Land Port of Entry Modernization: Promoting Security, Travel, and Trade | | 2015 |
| CBP | Law Enforcement Preemployment Test Alternative | | 2017 |
| CBP | Multi-year Investment and Management Plan - Inspection and Detection Technology | | 2016 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| Component/ Office | Appropriations Reports Required by Congress | Statutorily Recurring | Fiscal Year Required |
|---|---|---|---|
| CBP | Online Detainee Locator System | | 2017 |
| CBP | Progress on Implementing GAO Recommendations on Unaccompanied Children | | 2017 |
| CBP | Real Property Inventory and Recapitalization Plan | | 2016 |
| CBP | Real Property Inventory Plan | | 2015 |
| CBP | Reimbursable Fee Agreements Fifth Semiannual | | 2015 |
| CBP | Reimbursable Fee Agreements Sixth Semiannual | | 2015 |
| CBP | Resource Optimization at the Ports of Entry | | 2015 |
| CBP | Resource Optimization at the Ports of Entry | | 2016 |
| CBP | Resource Optimization at the Ports of Entry | | 2017 |
| CBP | Search and Rescue Efforts | | 2017 |
| CBP | Search and Rescue Efforts for FY 2015 | | 2016 |
| CBP | Section 559 Pilot Program Activities | | 2015 |
| CBP | Section 559 Pilot Program Donations Acceptance | Yes | 2015 |
| CBP | Section 559 Pilot Program Donations Acceptance Annual Report | Yes | 2016 |
| CBP | Section 559 Pilot Program Donations Activities Annual Report | | 2016 |
| CBP | Sexual Abuse and Sexual Assault by CBP Employees Annual Report | | 2016 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| Component/ Office | Appropriations Reports Required by Congress | Statutorily Recurring | Fiscal Year Required |
|---|---|---|---|
| CBP | Short-Term Detention Standards and Oversight | | 2015 |
| CBP | Strategic Air and Marine Plan Update | | 2015 |
| CBP | Textile Transshipment Enforcement | | 2015 |
| CBP | Unattended Ground Sensor Spectrum Study | | 2017 |
| CBP | Unmanned Aircraft Systems Pilots | | 2016 |
| CBP | Unmanned Aircraft Systems Usage | | 2015 |
| CBP | Use of Unmanned Aircraft Systems in Joint Operations with State, Local, and Tribal Partners | | 2017 |
| CBP | USVI Services and Memorandum of Agreement | | 2015 |
| CBRNE | DHS Chemical, Biological, Radiological and Nuclear Functions Review Report | | 2015 |
| DNDO | DNDO Obligation and Hiring Plan - Q1 | | 2016 |
| DNDO | DNDO Obligation and Hiring Plan - Q2 | | 2016 |
| DNDO | DNDO Obligation and Hiring Plan - Q3 | | 2016 |
| DNDO | DNDO Obligation and Hiring Plan - Q4 | | 2016 |
| DNDO | Procurement Forecast Plan—Human Portable Radiation Detection Systems | | 2015 |
| FEMA | Disaster Contracts Quarterly Report FY 2015 Report to Congress - Q1 | Yes | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| Component/ Office | Appropriations Reports Required by Congress | Statutorily Recurring | Fiscal Year Required |
|---|---|---|---|
| FEMA | Disaster Contracts Quarterly Report FY 2015 Report to Congress - Q2 | Yes | 2015 |
| FEMA | Disaster Contracts Quarterly Report FY 2015 Report to Congress - Q3 | Yes | 2015 |
| FEMA | Disaster Contracts Quarterly Report FY 2015 Report to Congress - Q4 | Yes | 2015 |
| FEMA | Disaster Contracts Quarterly Report FY 2016 Report to Congress - Q1 | Yes | 2016 |
| FEMA | Disaster Contracts Quarterly Report FY 2016 Report to Congress - Q2 | Yes | 2016 |
| FEMA | Disaster Contracts Quarterly Report FY 2016 Report to Congress - Q3 | Yes | 2016 |
| FEMA | Disaster Contracts Quarterly Report FY 2016 Report to Congress - Q4 | Yes | 2016 |
| FEMA | Disaster Contracts Quarterly Report FY 2017 Report to Congress - Q1 | Yes | 2017 |
| FEMA | Disaster Contracts Quarterly Report FY 2017 Report to Congress - Q2 | Yes | 2017 |
| FEMA | Disaster Contracts Quarterly Report FY 2017 Report to Congress - Q3 | Yes | 2017 |
| FEMA | Disaster Contracts Quarterly Report FY 2017 Report to Congress - Q4 | Yes | 2017 |
| FEMA | Disaster Readiness and Support: Quarterly Obligations - Q1 | | 2015 |
| FEMA | Disaster Readiness and Support: Quarterly Obligations - Q2 | | 2015 |
| FEMA | Disaster Relief Fund: FY 2016 Funding Requirements | Yes | 2015 |
| FEMA | Disaster Relief Fund: FY 2017 Funding Requirements | Yes | 2016 |
| FEMA | Disaster Relief Fund: FY 2018 Funding Requirements | Yes | 2017 |
| FEMA | DRF Fiscal Preparation for Disaster Costs | | 2017 |
| FEMA | DRF Monthly Report 1 - October 2014 | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| Component/ Office | Appropriations Reports Required by Congress | Statutorily Recurring | Fiscal Year Required |
|---|---|---|---|
| FEMA | DRF Monthly Report 1 - October 2015 | | 2016 |
| FEMA | DRF Monthly Report 1 - October 2016 | | 2017 |
| FEMA | DRF Monthly Report 10 - July 2015 | | 2015 |
| FEMA | DRF Monthly Report 10 - July 2016 | | 2016 |
| FEMA | DRF Monthly Report 10 - July 2017 | | 2017 |
| FEMA | DRF Monthly Report 11 - August 2015 | | 2015 |
| FEMA | DRF Monthly Report 11 - August 2016 | | 2016 |
| FEMA | DRF Monthly Report 11 - August 2017 | | 2017 |
| FEMA | DRF Monthly Report 12 - September 2015 | | 2015 |
| FEMA | DRF Monthly Report 12 - September 2016 | | 2016 |
| FEMA | DRF Monthly Report 12 - September 2017 | | 2017 |
| FEMA | DRF Monthly Report 2 - November 2014 | | 2015 |
| FEMA | DRF Monthly Report 2 - November 2015 | | 2016 |
| FEMA | DRF Monthly Report 2 - November 2016 | | 2017 |
| FEMA | DRF Monthly Report 3 - December 2014 | | 2015 |
| FEMA | DRF Monthly Report 3 - December 2015 | | 2016 |
| FEMA | DRF Monthly Report 3 - December 2016 | | 2017 |
| FEMA | DRF Monthly Report 4 - January 2015 | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| FEMA | DRF Monthly Report 4 - January 2016 | | 2016 |
| FEMA | DRF Monthly Report 4 - January 2017 | | 2017 |
| FEMA | DRF Monthly Report 5 - February 2015 | | 2015 |
| FEMA | DRF Monthly Report 5 - February 2016 | | 2016 |
| FEMA | DRF Monthly Report 5 - February 2017 | | 2017 |
| FEMA | DRF Monthly Report 6 - March 2015 | | 2015 |
| FEMA | DRF Monthly Report 6 - March 2016 | | 2016 |
| FEMA | DRF Monthly Report 6 - March 2017 | | 2017 |
| FEMA | DRF Monthly Report 7 - April 2015 | | 2015 |
| FEMA | DRF Monthly Report 7 - April 2016 | | 2016 |
| FEMA | DRF Monthly Report 7 - April 2017 | | 2017 |
| FEMA | DRF Monthly Report 8 - May 2015 | | 2015 |
| FEMA | DRF Monthly Report 8 - May 2016 | | 2016 |
| FEMA | DRF Monthly Report 8 - May 2017 | | 2017 |
| FEMA | DRF Monthly Report 9 - June 2015 | | 2015 |
| FEMA | DRF Monthly Report 9 - June 2016 | | 2016 |
| FEMA | DRF Monthly Report 9 - June 2017 | | 2017 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| FEMA | Effectiveness of the Program to Prepare Communities for Complex Coordinated Terrorist Attacks and the Countering Violent Extremism Grant Program | | 2017 |
| FEMA | Emergency Food and Shelter Joint Transition Plan | | 2016 |
| FEMA | Emergency Operations Center Interconnectedness | | 2017 |
| FEMA | Ensuring Rail Security | | 2017 |
| FEMA | FEMA Obligation and Hiring Plan - Q1 | | 2016 |
| FEMA | FEMA Obligation and Hiring Plan - Q2 | | 2016 |
| FEMA | FEMA Obligation and Hiring Plan - Q3 | | 2016 |
| FEMA | FEMA Obligation and Hiring Plan - Q4 | | 2016 |
| FEMA | Grant Expenditures on the Needs of Children in Disasters | | 2015 |
| FEMA | Impact of Length of Claims Adjustment Process on Administrative Costs of Disasters | | 2015 |
| FEMA | Individual Assistance for Cooperatives and Condominiums | | 2016 |
| FEMA | Law Enforcement Terrorism Prevention Program Expenditures | | 2015 |
| FEMA | MWEOC Capital Infrastructure Investment Plan | | 2017 |
| FEMA | National Pre-Disaster Mitigation Fund | | 2017 |
| FEMA | One Risk Premium Rate Table | | 2017 |
| FEMA | Overview of Risk MAP CNMS and NVUE Status | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| FEMA | Public Assistance Program Alternative Procedures - Q1 | | 2015 |
| FEMA | Public Assistance Program Alternative Procedures - Q2 | | 2015 |
| FEMA | Public Assistance Program Alternative Procedures - Q3 | | 2015 |
| FEMA | Public Assistance Program Alternative Procedures - Q4 | | 2015 |
| FEMA | Rolling Grants Deadlines | | 2015 |
| FEMA | Technical Mapping Assistance Committee | | 2015 |
| FLETC | 2015 Update to the 2010 FLETC Comprehensive Master Plan | | 2015 |
| FLETC | FLETC Obligation and Hiring Plan - Q1 | | 2016 |
| FLETC | FLETC Obligation and Hiring Plan - Q2 | | 2016 |
| FLETC | FLETC Obligation and Hiring Plan - Q3 | | 2016 |
| FLETC | FLETC Obligation and Hiring Plan - Q4 | | 2016 |
| I&A/OPS | I&A Obligation and Hiring Plan - Q1 | | 2016 |
| I&A/OPS | I&A Obligation and Hiring Plan - Q2 | | 2016 |
| I&A/OPS | I&A Obligation and Hiring Plan - Q3 | | 2016 |
| I&A/OPS | I&A Obligation and Hiring Plan - Q4 | | 2016 |
| ICE | Alternatives to Detention - First Semiannual FY 2017 | | 2017 |
| ICE | Alternatives to Detention - Second Semiannual FY 2017 | | 2017 |
| ICE | Anti-Trafficking Coordination Teams | | 2016 |
| ICE | Comprehensive Plan for Immigration Data Improvement | | 2017 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| ICE | Comprehensive Strategy for Overstay Enforcement and Deterrence | | 2017 |
| ICE | Deportation of Parents Claiming U.S.-Born Children – CY 2015 First Half | | 2015 |
| ICE | Deportation of Parents Claiming U.S.-Born Children – CY 2015 Second Half | | 2015 |
| ICE | Deportation of Parents Claiming U.S.-Born Children – CY 2016 First Half | | 2016 |
| ICE | Deportation of Parents Claiming U.S.-Born Children – CY 2016 Second Half | | 2016 |
| ICE | Deportation of Parents Claiming U.S.-Born Children – CY 2017 First Half | | 2017 |
| ICE | Deportation of Parents Claiming U.S.-Born Children – CY 2017 Second Half | | 2017 |
| ICE | Detention and Removal of Gang Members | | 2016 |
| ICE | Detention Bed Capacity | | 2017 |
| ICE | Detention Requests - Q1 and Q2 | | 2017 |
| ICE | Detention Requests - Q3 | | 2017 |
| ICE | Detention Requests - Q4 | | 2017 |
| ICE | Forced Labor and Forced Child Labor | | 2017 |
| ICE | HSI Human Trafficking and Victim Assistance Programs | | 2017 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| ICE | ICE Notification of Non-PBNDS Detention Contract (Jerome County) | | 2017 |
| ICE | ICE Notification of Non-PBNDS Detention Contract (Nye County) | | 2017 |
| ICE | ICE Notification of Non-PBNDS Detention Contract (Sherburne County) | | 2017 |
| ICE | ICE Notification of Non-PBNDS Detention Contract (Webb County) | | 2017 |
| ICE | ICE Obligation and Hiring Plan - Q1 | | 2016 |
| ICE | ICE Obligation and Hiring Plan - Q2 | | 2016 |
| ICE | ICE Obligation and Hiring Plan - Q3 | | 2016 |
| ICE | ICE Obligation and Hiring Plan - Q4 | | 2016 |
| ICE | Illegal Trafficking of Wildlife and Other Natural Resources | | 2016 |
| ICE | Illegal Trafficking of Wildlife and Other Natural Resources | | 2017 |
| ICE | Office of Information Technology Multi-Year Investment and Management Plan | | 2015 |
| ICE | Operational Resources in the Caribbean | | 2015 |
| ICE | Progress in Implementing 2011 PBNDS Standards and DHS PREA Requirements at Detention Facilities | | 2017 |
| ICE | Progress in Implementing Performance-Based National Detention Standards | | 2016 |
| ICE | Release of Detainees in Fiscal Year 2013 | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| ICE | State Crime Labs | | 2017 |
| ICE | State Police Crime Lab Support | | 2016 |
| ICE | Visa Overstay Enforcement Investigations Expenditure Plan | | 2016 |
| MGMT/OCFO/ Budget | Common Appropriations Structure - Technical Assistance, Certification, Plan, FMPM | | 2016 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 1 - October 2016 | | 2017 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 1 – October 2014 | | 2015 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 1 - October 2015 | | 2016 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 10 - July 2015 | | 2015 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 10 - July 2016 | | 2016 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 10 - July 2017 | | 2017 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 11 - August 2015 | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 11 - August 2016 | | 2016 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 11 - August 2017 | | 2017 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 12 - September 2015 | | 2015 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 12 - September 2016 | | 2016 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 12 - September 2017 | | 2017 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 2 - November 2014 | | 2015 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 2 - November 2015 | | 2016 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 2 - November 2016 | | 2017 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 3 - December 2014 | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 3 - December 2015 | | 2016 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 3 - December 2016 | | 2017 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 4 - January 2015 | | 2015 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 4 - January 2016 | | 2016 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 4 - January 2017 | | 2017 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 5 - February 2015 | | 2015 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 5 - February 2016 | | 2016 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 5 - February 2017 | | 2017 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 6 - March 2015 | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 6 - March 2016 | | 2016 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 6 - March 2017 | | 2017 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 7 - April 2015 | | 2015 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 7 - April 2016 | | 2016 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 7 - April 2017 | | 2017 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 8 - May 2015 | | 2015 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 8 - May 2016 | | 2016 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 8 - May 2017 | | 2017 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 9 - June 2015 | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 9 - June 2016 | | 2016 |
| MGMT/OCFO/ Budget | Monthly Budget Execution and Staffing Report 9 - June 2017 | | 2017 |
| MGMT/OCFO/ Budget | Quarterly Execution Report - Q1 and Q2 | | 2017 |
| MGMT/OCFO/ Budget | Quarterly Execution Report - Q3 | | 2017 |
| MGMT/OCFO/ Budget | Quarterly Execution Report - Q4 | | 2017 |
| MGMT/OCFO/ Budget | Reduction of Printing and Reproduction Costs | | 2016 |
| MGMT/OCFO/ GAO-OIG Liaison | Grants and Contracts Awarded by Means Other than Full and Open Competition | Yes | 2016 |
| MGMT/OCFO/ OFM | Conference Spending | Yes | 2016 |
| MGMT/OCFO/ OFM | Conference Spending | Yes | 2017 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| MGMT/OCFO/ OFM | DHS Collection of Conference Fees from Non-Federal Participants in DHS Conferences: FY 2015 | Yes | 2015 |
| MGMT/OCFO/ OFM | DHS Collection of Conference Fees from Non-Federal Participants in DHS Conferences: FY 2015 and 2016 | Yes | 2016 |
| MGMT/OCFO/ OFM | DHS Collection of Conference Fees from Non-Federal Participants in DHS Conferences: FY 2017 | Yes | 2017 |
| MGMT/OCFO/ OFM | Grants or Contracts | | 2017 |
| MGMT/OCFO/ OFO | A Common Appropriations Structure for DHS: FY 2016 Crosswalk | | 2015 |
| MGMT/OCFO/ OFO | Bonuses and Performance Awards | | 2016 |
| MGMT/OCFO/ OFO | DHS Financial Systems Modernization Expenditure Plan | | 2015 |
| MGMT/OCFO/ OFO | Expenditure Plan - OSEM | | 2016 |
| MGMT/OCFO/ OFO | Financial Systems Modernization | | 2017 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| MGMT/OCFO/ OFO | Obligation and Hiring Plan (MGMT) - Q1 | | 2016 |
| MGMT/OCFO/ OFO | Obligation and Hiring Plan (MGMT) - Q2 | | 2016 |
| MGMT/OCFO/ OFO | Obligation and Hiring Plan (MGMT) - Q3 | | 2016 |
| MGMT/OCFO/ OFO | Obligation and Hiring Plan (MGMT) - Q4 | | 2016 |
| MGMT/OCFO/ OFO | Obligation and Hiring Plan (OSEM) - Q1 | | 2016 |
| MGMT/OCFO/ OFO | Obligation and Hiring Plan (OSEM) - Q2 | | 2016 |
| MGMT/OCFO/ OFO | Obligation and Hiring Plan (OSEM) - Q3 | | 2016 |
| MGMT/OCFO/ OFO | Obligation and Hiring Plan (OSEM) - Q4 | | 2016 |
| MGMT/OCFO/ OFO | Official Reception and Representation Expenses - Q1 | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| MGMT/OCFO/ OFO | Official Reception and Representation Expenses - Q2 | | 2015 |
| MGMT/OCFO/ OFO | Official Reception and Representation Expenses - Q3 | | 2015 |
| MGMT/OCFO/ OFO | Official Reception and Representation Expenses - Q4 | | 2015 |
| MGMT/OCFO/ OFO | Official Reception and Representation Expenses - Quarter 1 | | 2016 |
| MGMT/OCFO/ OFO | Official Reception and Representation Expenses - Quarter 2 | | 2016 |
| MGMT/OCFO/ OFO | Official Reception and Representation Expenses - Quarter 3 | | 2016 |
| MGMT/OCFO/ OFO | Official Reception and Representation Expenses - Quarter 4 | | 2016 |
| MGMT/OCFO/ OFO | Purchase and Usage of Ammunition | Yes | 2015 |
| MGMT/OCFO/ OFO | Purchase and Usage of Ammunition | Yes | 2016 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| MGMT/OCFO/ OFO | Purchase and Usage of Ammunition and Weapons | Yes | 2017 |
| MGMT/OCFO/ OFO | Purchase and Usage of Weapons - CY 2015 | Yes | 2016 |
| MGMT/OCFO/ OFO | Reception and Representation Expenses - Q1 | | 2017 |
| MGMT/OCFO/ OFO | Reception and Representation Expenses - Q2 | | 2017 |
| MGMT/OCFO/ OFO | Reception and Representation Expenses - Q3 | | 2017 |
| MGMT/OCFO/ OFO | Reception and Representation Expenses - Q4 | | 2017 |
| MGMT/OCFO/ OFO | S1/S2 Travel - Q1 and Q2 | | 2017 |
| MGMT/OCFO/ OFO | S1/S2 Travel - Q3 | | 2017 |
| MGMT/OCFO/ OFO | S1/S2 Travel - Q4 | | 2017 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| MGMT/OCFO/ OFO | Travel for Secretary and Deputy Secretary - Q1 | | 2015 |
| MGMT/OCFO/ OFO | Travel for Secretary and Deputy Secretary - Q2 | | 2015 |
| MGMT/OCFO/ OFO | Travel for Secretary and Deputy Secretary - Q3 | | 2015 |
| MGMT/OCFO/ OFO | Travel for Secretary and Deputy Secretary - Q4 | | 2015 |
| MGMT/OCFO/ OFO | Travel for Secretary and Deputy Secretary - Quarter 1 | | 2016 |
| MGMT/OCFO/ OFO | Travel for Secretary and Deputy Secretary - Quarter 2 | | 2016 |
| MGMT/OCFO/ OFO | Working Capital Fund - Q1 | | 2015 |
| MGMT/OCFO/ OFO | Working Capital Fund - Q1 | | 2016 |
| MGMT/OCFO/ OFO | Working Capital Fund - Q1 | | 2017 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| MGMT/OCFO/ OFO | Working Capital Fund - Q2 | | 2015 |
| MGMT/OCFO/ OFO | Working Capital Fund - Q2 | | 2016 |
| MGMT/OCFO/ OFO | Working Capital Fund - Q2 | | 2017 |
| MGMT/OCFO/ OFO | Working Capital Fund - Q3 | | 2015 |
| MGMT/OCFO/ OFO | Working Capital Fund - Q3 | | 2016 |
| MGMT/OCFO/ OFO | Working Capital Fund - Q3 | | 2017 |
| MGMT/OCFO/ OFO | Working Capital Fund - Q4 | | 2015 |
| MGMT/OCFO/ OFO | Working Capital Fund - Q4 | | 2016 |
| MGMT/OCFO/ OFO | Working Capital Fund - Q4 | | 2017 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| MGMT/OCFO/ PA&E | Future Years Homeland Security Program | Yes | 2015 |
| MGMT/OCFO/ PA&E | Future Years Homeland Security Program | Yes | 2016 |
| MGMT/OCFO/ PAE | Future Years Homeland Security Program | Yes | 2017 |
| MGMT/OCHCO | Administratively Uncontrollable Overtime (AUO) Compliance Plans | | 2015 |
| MGMT/OCHCO | Hiring Delays - Q2 (combined FY 2015 Q2, Q3, and Q4) | | 2015 |
| MGMT/OCHCO | Hiring Delays - Q3 (combined FY 2015 Q2, Q3, and Q4) | | 2015 |
| MGMT/OCHCO | Hiring Delays - Q4 (combined FY 2015 Q2, Q3, and Q4) | | 2015 |
| MGMT/OCHCO | Strategy to Reduce the Time to Hire Q1 | | 2015 |
| MGMT/OCIO | Cybersecurity Improvements Expenditure Plan Obligations - First Half, FY 2016 | | 2016 |
| MGMT/OCIO | Cybersecurity Improvements Expenditure Plan Obligations - Second Half, FY 2016 | | 2016 |
| MGMT/OCIO | Information Technology System Vulnerabilities Expenditure Report | | 2015 |
| MGMT/OCRSO | DHS Consolidated Headquarters FY 2015 Expenditure Plan | | 2015 |
| MGMT/OCRSO | DHS Field Efficiencies Implementation Plan | | 2017 |
| MGMT/OCRSO | Disposition of Plum Island | | 2016 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| MGMT/OCRSO | Headquarters Consolidation Expenditure Plan | | 2016 |
| MGMT/OCSO | Document Security | | 2015 |
| MGMT/PARM | CASR - Q1 Update | | 2015 |
| MGMT/PARM | CASR - Q1 Update | | 2016 |
| MGMT/PARM | CASR - Q2 Update | | 2015 |
| MGMT/PARM | CASR - Q2 Update | | 2016 |
| MGMT/PARM | CASR - Q3 Update | | 2015 |
| MGMT/PARM | CASR - Q3 Update | | 2016 |
| MGMT/PARM | Comprehensive Acquisition Status Annual Report (CASR) - FY 2014 | | 2015 |
| MGMT/PARM | Comprehensive Acquisition Status Annual Report (CASR) - FY 2015 | | 2016 |
| NPPD | 5-Year Real Property Plan | | 2017 |
| NPPD | CFATS Implementation Semiannual Report - First Half - FY 2016 | | 2016 |
| NPPD | CFATS Implementation Semiannual Report - Second Half - FY 2016 | | 2016 |
| NPPD | Continuous Diagnostics and Mitigation Obligation and Expenditure Report Q1 & Q2, FY 2015 | | 2015 |
| NPPD | Continuous Diagnostics and Mitigation Obligation and Expenditure Report Q3, FY 2015 | | 2015 |
| NPPD | Continuous Diagnostics and Mitigation Obligation and Expenditure Report Q4, FY 2015 | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| NPPD | Critical Infrastructure Activities | | 2015 |
| NPPD | Defense/Non-Defense Classification | | 2017 |
| NPPD | Enhanced Cybersecurity Services | | 2016 |
| NPPD | Enhanced Cybersecurity Services Program | | 2015 |
| NPPD | FPS Certification of Full Funding | | 2016 |
| NPPD | FPS Strategic Human Capital Plan | | 2015 |
| NPPD | FPS Strategic Human Capital Plan | | 2016 |
| NPPD | Implementation Status of the Chemical Facility Anti-Terrorism Standards First Half, FY 2015 | | 2015 |
| NPPD | Implementation Status of the Chemical Facility Anti-Terrorism Standards Second Half, FY 2015 | | 2015 |
| NPPD | Intrusions of Information Systems and Critical Infrastructure | | 2017 |
| NPPD | National Emergency Communications Plan Status Report | | 2016 |
| NPPD | Network Security Deployment Obligation and Expenditure Report Q1 & Q2, FY 2015 | | 2015 |
| NPPD | Network Security Deployment Obligation and Expenditure Report Q3, FY 2015 | | 2015 |
| NPPD | Network Security Deployment Obligation and Expenditure Report Q4, FY 2015 | | 2015 |

| | |
|---|---|
| Question#: | 13 |
| Topic: | Internal Reports |
| Hearing: | Mitigating America's Cybersecurity Risk |
| Primary: | The Honorable Rand Paul |
| Committee: | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| NPPD | NPPD Obligation and Hiring Plan - Q1 | | 2016 |
| NPPD | NPPD Obligation and Hiring Plan - Q2 | | 2016 |
| NPPD | NPPD Obligation and Hiring Plan - Q3 | | 2016 |
| NPPD | NPPD Obligation and Hiring Plan - Q4 | | 2016 |
| NPPD | Office of Biometric Identity Management Expenditure Plan Q1 & Q2 | | 2015 |
| NPPD | Office of Biometric Identity Management Expenditure Plan Q3 | | 2015 |
| NPPD | Office of Biometric Identity Management Expenditure Plan Q4 | | 2015 |
| NPPD | Office of Biometric Identity Management Multi-Year Investment and Management Plan | | 2015 |
| NPPD | Rural Emergency Medical Communications Demonstration Project | | 2016 |
| NPPD | Strategic Plan on Infrastructure Protection Assessments | | 2016 |
| NPPD | Strategic Plan to Ensure Civilian Federal Networks | | 2017 |
| OHA | Advancing Bioterrorism Detection Capabilities | | 2017 |
| OHA | OHA Obligation and Hiring Plan - Q1 | | 2016 |
| OHA | OHAObligation and Hiring Plan - Q2 | | 2016 |
| OHA | OHAObligation and Hiring Plan - Q3 | | 2016 |
| OHA | OHAObligation and Hiring Plan - Q4 | | 2016 |
| OIG | Expenditure Plan - FY 2016 | | 2016 |
| OIG | Expenditure Plan - FY 2017 | | 2016 |

|  |  |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

|  |  |  |  |
|---|---|---|---|
| OIG | Grants or Contracts |  | 2017 |
| OIG | OIG Obligation and Hiring Plan - Q1 |  | 2016 |
| OIG | OIG Obligation and Hiring Plan - Q2 |  | 2016 |
| OIG | OIG Obligation and Hiring Plan - Q3 |  | 2016 |
| OIG | OIG Obligation and Hiring Plan - Q4 |  | 2016 |
| OIG/CBP/ICE | Investigation of DHS Employee Corruption Cases |  | 2015 |
| OPS | Operations Centers across the Department of Homeland Security |  | 2015 |
| OSEM/OPE | DHS Countering Violent Extremism Programs and Initiatives |  | 2017 |
| OSEM/OPE/ OCP | Countering Violent Extremism Programs and Initiatives |  | 2016 |
| OSEM/PLCY | Cooperation with Mexican Authorities |  | 2017 |
| OSEM/PLCY | FY 2015 Border Security Status Report - Q1 |  | 2015 |
| OSEM/PLCY | FY 2015 Border Security Status Report - Q2 |  | 2015 |
| OSEM/PLCY | FY 2015 Border Security Status Report - Q3 |  | 2015 |
| OSEM/PLCY | FY 2015 Border Security Status Report - Q4 |  | 2015 |
| OSEM/PLCY | FY 2016 Border Security Status Report - Q1 |  | 2016 |
| OSEM/PLCY | FY 2016 Border Security Status Report - Q2 |  | 2016 |
| OSEM/PLCY | FY 2016 Border Security Status Report - Q3 |  | 2016 |
| OSEM/PLCY | FY 2016 Border Security Status Report - Q4 |  | 2016 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| OSEM/PLCY | FY 2017 Border Security Status Report - Q1 | | 2017 |
| OSEM/PLCY | FY 2017 Border Security Status Report - Q2 | | 2017 |
| OSEM/PLCY | FY 2017 Border Security Status Report - Q3 | | 2017 |
| OSEM/PLCY | FY 2017 Border Security Status Report - Q4 | | 2017 |
| OSEM/PLCY | Inadmissibility of Tax-Based Citizenship Renunciants | | 2015 |
| OSEM/PLCY | Overseas Personnel | | 2017 |
| OSEM/PLCY | Stolen and Lost Travel Documents | | 2015 |
| OSEM/PLCY | Stolen and Lost Travel Documents | | 2016 |
| OSEM/PLCY | Use of International Mobile Subscriber Identity Catcher Technology | | 2017 |
| S&T | Countering Cyber Threats through Technical Cooperation with the Department of Defense | | 2015 |
| S&T | DHS S&T Component Liaison Program | | 2015 |
| S&T | Improved Situational Awareness at the Border Plan | | 2015 |
| S&T | Metrics Used to Make DHS Center of Excellence Awards | | 2015 |
| S&T | NBAF Construction Plan Update | | 2016 |
| S&T | Prophylactic Ionizing Radiation Protection Capability | | 2015 |
| S&T | Research and Development Results | | 2016 |
| S&T | Results of Fiscal Year 2014 Research and Development | | 2015 |
| S&T | S&T Obligation and Hiring Plan - Q1 | | 2016 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| S&T | S&T Obligation and Hiring Plan - Q2 | | 2016 |
| S&T | S&T Obligation and Hiring Plan - Q3 | | 2016 |
| S&T | S&T Obligation and Hiring Plan - Q4 | | 2016 |
| S&T | S&T Reforms: Integrated Product Teams and Technical Assessments | | 2015 |
| TSA | Advanced Integrated Passenger and Baggage Screening Technologies | Yes | 2015 |
| TSA | Advanced Integrated Passenger Screening Technologies | Yes | 2016 |
| TSA | Advanced Integrated Passenger Screening Technologies | Yes | 2017 |
| TSA | Expedited Passenger Screening First Half, FY 2015 | | 2015 |
| TSA | Expedited Passenger Screening Second Half, FY 2015 | | 2015 |
| TSA | FAMS Mission Coverage, Staffing, and Hiring - Q1 | | 2015 |
| TSA | FAMS Mission Coverage, Staffing, and Hiring - Q1 | | 2016 |
| TSA | FAMS Mission Coverage, Staffing, and Hiring - Q1 | | 2017 |
| TSA | FAMS Mission Coverage, Staffing, and Hiring - Q2 | | 2015 |
| TSA | FAMS Mission Coverage, Staffing, and Hiring - Q2 | | 2016 |
| TSA | FAMS Mission Coverage, Staffing, and Hiring - Q2 | | 2017 |
| TSA | FAMS Mission Coverage, Staffing, and Hiring - Q3 | | 2015 |
| TSA | FAMS Mission Coverage, Staffing, and Hiring - Q3 | | 2016 |
| TSA | FAMS Mission Coverage, Staffing, and Hiring - Q3 | | 2017 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| TSA | FAMS Mission Coverage, Staffing, and Hiring - Q4 | | 2015 |
| TSA | FAMS Mission Coverage, Staffing, and Hiring - Q4 | | 2016 |
| TSA | FAMS Mission Coverage, Staffing, and Hiring - Q4 | | 2017 |
| TSA | Future FAMS Staffing Requirements | | 2015 |
| TSA | FY 2014 Unclaimed Money at Airports | Yes | 2015 |
| TSA | FY 2015 FAMS Expenditure and Staffing Plan | | 2015 |
| TSA | FY 2015 Unclaimed Money at Airports | Yes | 2016 |
| TSA | FY 2016 Unclaimed Money at Airports | Yes | 2017 |
| TSA | National Explosives Detection Canine Team Program | | 2016 |
| TSA | Recoveries and Deobligations - Semiannual 1 | Yes | 2017 |
| TSA | Recoveries and Deobligations - Semiannual 2 | Yes | 2017 |
| TSA | Recoveries and Deobligations First Half, FY 2015 | Yes | 2015 |
| TSA | Reimbursement Plan for Baggage Screening Systems Outstanding Claims | | 2016 |
| TSA | Responses to Government Accountability Office (GAO) Recommendations Outlined in GAO-14-357, "Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next-Generation Systems" | | 2015 |
| TSA | Scientific Substantiation of Behavioral Indicators | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| TSA | Screening Partnership Program First Half, FY 2015 | | 2015 |
| TSA | Screening Partnership Program Second Half, FY 2015 | | 2015 |
| TSA | Semiannual Recoveries and Deobligations - Second Half | Yes | 2016 |
| TSA | SIDA Airport Security | | 2017 |
| TSA | Transport of Security-Sensitive Materials First Half, FY 2015 | | 2015 |
| TSA | Transport of Security-Sensitive Materials Second Half, FY 2015 | | 2015 |
| TSA | Transportation Sector Security Risk Assessment | | 2015 |
| TSA | TSA Obligation and Hiring Plan - Q1 | | 2016 |
| TSA | TSA Obligation and Hiring Plan - Q2 | | 2016 |
| TSA | TSA Obligation and Hiring Plan - Q3 | | 2016 |
| TSA | TSA Obligation and Hiring Plan - Q4 | | 2016 |
| TSA | Uniforms Procurement: Compliance with the Buy American Act | | 2015 |
| USCG | Alaskan Asset Replacement Plan and Coverage | | 2017 |
| USCG | Arctic Icebreaking Capabilities | | 2016 |
| USCG | Arctic Search and Rescue | | 2017 |
| USCG | Bering Sea and Arctic Ocean Response | | 2017 |
| USCG | Bering Sea and Arctic Region Coverage | | 2016 |
| USCG | Boat Expenditure Plan | | 2015 |
| USCG | Boat Expenditure Plan | | 2017 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| USCG | Coast Guard Concept of Operations for Offshore Assets | | 2016 |
| USCG | Coast Guard Mission Needs Statement | | 2015 |
| USCG | Coast Guard Yard Dry-dock Facilities and Industrial Equipment | | 2015 |
| USCG | Commercial Fishing Safety Training Grant Program | | 2017 |
| USCG | Electronic Aids to Navigation | | 2016 |
| USCG | Environmental Compliance and Restoration Backlog Report | | 2015 |
| USCG | Environmental Compliance and Restoration Projects Backlog Report | | 2016 |
| USCG | Great Lakes Icebreaking Mission Analysis | | 2016 |
| USCG | Gulf of Mexico Oil Production Platform: Discharge Activities | | 2015 |
| USCG | Military Housing Resolution of Deficiencies Report | | 2015 |
| USCG | Minor Shore Infrastructure Projects and Military Housing Expenditure Plan | | 2015 |
| USCG | Pilot Training Program on Fishing Safety | | 2016 |
| USCG | Polar Icebreaker Requirements | | 2017 |
| USCG | Sexual Assaults: Expedited Transfer and Special Victims Counsel Program | Yes | 2015 |
| USCG | Sexual Assaults: Expedited Transfer and Special Victims Counsel Program | Yes | 2017 |
| USCG | Sexual Assaults: Expedited Transfer and Special Victims Counsel Program | Yes | 2016 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| USCG | Small Boat Activities - FY 2016 | | 2016 |
| USCG | Unmanned Aircraft Systems: Acquisition and Utilization | | 2016 |
| USCG | USCG FY 2016 Capital Investment Plan | Yes | 2015 |
| USCG | USCG FY 2017 Capital Investment Plan | Yes | 2016 |
| USCG | USCG FY 2018 Capital Investment Plan | Yes | 2017 |
| USCG | USCG Minor Construction Projects - FY 2016 | | 2016 |
| USCG | USCG Minor Construction Projects (FY 2017) | | 2016 |
| USCG | USCG Minor Construction Projects (FY 2018) | | 2017 |
| USCG | USCG Obligation and Hiring Plan - Q1 | | 2016 |
| USCG | USCG Obligation and Hiring Plan - Q2 | | 2016 |
| USCG | USCG Obligation and Hiring Plan - Q3 | | 2016 |
| USCG | USCG Obligation and Hiring Plan - Q4 | | 2016 |
| USCG | USCG Unfunded Priorities | | 2016 |
| USCG | USCG Unfunded Priorities | | 2015 |
| USCIS | Advance Parole | | 2016 |
| USCIS | Affirmative Asylum Application Statistics and Decisions Annual Report | | 2016 |
| USCIS | Cost Associated with U.S. Refugee Admissions Program [USRAP] | | 2017 |
| USCIS | EB-5 Visa Program First Half, FY 2015 | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| USCIS | EB-5 Visa Program Second Semiannual, FY 2015 | | 2015 |
| USCIS | Employment Authorization Documents | | 2017 |
| USCIS | Estimated Costs and Timeline to Implement Mandatory E-Verify - FY 2016 | | 2016 |
| USCIS | H-1B and L Compliance Review Site Visits | | 2017 |
| USCIS | H-1B and L-1A Compliance Review Site Visits | | 2016 |
| USCIS | H-2B Usage and Recommendations | | 2016 |
| USCIS | Individuals Receiving Benefits Under TPS | | 2017 |
| USCIS | Integrity of O–1B and O–2 Visa Issuances | | 2016 |
| USCIS | Quinquennial Report on Asylum Decision Trends and Factors | Yes | 2016 |
| USCIS | Site Visit Programs/National Security Compliance Audits | | 2016 |
| USCIS | USCIS Fee Waiver Policies and Data | | 2017 |
| USCIS | USCIS Obligation and Hiring Plan - Q1 | | 2016 |
| USCIS | USCIS Obligation and Hiring Plan - Q2 | | 2016 |
| USCIS | USCIS Obligation and Hiring Plan - Q3 | | 2016 |
| USCIS | USCIS Obligation and Hiring Plan - Q4 | | 2016 |
| USCIS | USCIS Service Center Operations | | 2016 |
| USSS | Facilities Funding Obligation Plan | | 2016 |
| USSS | Human Capital Plan (FY 2015 – FY 2019) | | 2015 |

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | Internal Reports |
| **Hearing:** | Mitigating America's Cybersecurity Risk |
| **Primary:** | The Honorable Rand Paul |
| **Committee:** | HOMELAND SECURITY (SENATE) |

| | | | |
|---|---|---|---|
| USSS | James J. Rowley Training Center Capital Infrastructure Investment Plan | | 2016 |
| USSS | James J. Rowley Training Center Revised Master Plan | | 2016 |
| USSS | Professionalism within the Workforce | | 2015 |
| USSS | USSS Obligation and Hiring Plan - Q1 | | 2016 |
| USSS | USSS Obligation and Hiring Plan - Q2 | | 2016 |
| USSS | USSS Obligation and Hiring Plan - Q3 | | 2016 |
| USSS | USSS Obligation and Hiring Plan - Q4 | | 2016 |

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

**441 G St. N.W.**
**Washington, DC 20548**

June 15, 2018

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
U.S. Senate

**Subject: GAO Responses to Questions for the Record on the April 24, 2018 Hearing on Mitigating America's Cybersecurity Risks**

This letter responds to your May 10, 2018 request that I reply to additional questions arising from the Committee on Homeland Security and Governmental Affairs hearing on mitigating cybersecurity risks at the Department of Homeland Security (DHS). The enclosure provides my responses.

Should you or your staff have any questions on the matters discussed in this letter, please contact me at (202) 512-6244 or wilshuseng@gao.gov.

Sincerely yours,

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Enclosure

## Senate Committee on Homeland Security and Governmental Affairs

## Committee Hearing:
## Mitigating America's Cybersecurity Risks

## Questions for the Record

### Questions for the Record from Ranking Member Claire McCaskill
### Committee on Homeland Security and Governmental Affairs

1. **Has GAO tracked how many federal agencies have fully implemented any phase of CDM? If so, what is the breakdown of federal agencies and what phase of CDM is fully operational within each one?**

   We have not tracked how many federal agencies have fully implemented any phase of the continuous diagnostics and mitigation (CDM) program and do not have a breakdown of federal agencies that indicates what phase of CDM is fully operational within each agency.[1] However, in May 2016, we reported that most of the 17 civilian agencies covered by the Chief Financial Officers (CFO) Act that had high-impact systems were in the early stages of implementing CDM.[2] For example, 14 of the 17 agencies that we surveyed indicated that they had deployed phase 1 products to automate hardware and software asset configuration settings and common vulnerability management. Two of the 17 agencies responded that they had completed installation of agency and bureau/component-level dashboards and monitored attributes of authorized users operating in their agency's computing environment. More recently, in March 2018, the Office of Management and Budget reported that nearly 20 agencies now report data in near-real-time to their dashboards, after having deployed CDM phase 1 sensors and tools.[3]

   In response to a request from the Committee on Homeland Security and Governmental Affairs, we are planning to conduct a review of federal agencies' implementation of continuous monitoring programs. As part of that review, we intend to assess the extent to which each of the 23 civilian CFO Act agencies has implemented the CDM phases.[4] We expect to begin this review in early 2019.

[1] The CDM program aims to strengthen the cybersecurity of the federal government's networks at more than 65 participating agencies by providing tools and dashboards that continually monitor and report on network vulnerabilities. Tools are delivered in four phases: phase 1 and 2 tools report vulnerabilities in hardware and software, and user access controls, respectively; phase 3 tools will report on efforts to prevent attacks; and phase 4 tools will provide encryption to protect network data.

[2] GAO, Information Security: Agencies Need to Improve Controls Over Selected High-Impact Systems, GAO-16-501 (Washington, D.C.: May 18, 2016).

[3] Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2017*, (Washington, D.C.: March 2018).

[4] The Department of Defense (the 24th CFO Act agency) is not required to participate in the CDM program.

2. **What federal agencies are not participating in the CDM initiative and why?**

   To date, we have not conducted work that identified which federal agencies are not participating in the CDM initiative. As noted in the previous response, our planned review of continuous monitoring programs, requested by the Committee on Homeland Security and Government Affairs, is expected to determine the extent to which each of the 23 civilian CFO Act agencies are participating in the CDM initiative.

3. **Some critics of CDM dislike the blanket purchase agreement aspect of the program, saying it's not flexible enough to be useful. With the contract expiring this summer, does GAO have suggestions on how to address those concerns?**

   We have not assessed the blanket purchase agreement aspect of the CDM program and, thus, are not positioned to offer a view on the extent of its flexibility. However, in May 2018, we reported that the CDM program had changed its strategy for procuring CDM tools and integration services through the General Services Administration (GSA).[5] The CDM program previously issued task orders for the CDM tools and services through blanket purchase agreements established under vendors' GSA Federal Supply Schedule contracts. However, these agreements are set to expire in August 2018. Going forward, the program plans to use an existing GSA government-wide acquisition contract—known as Alliant—to obtain CDM tools and services.

   According to officials from the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD), the new acquisition strategy is intended to provide greater flexibility in contracting for current capabilities and to support future capabilities. It is also intended to allow participating agencies to order additional CDM-approved products or services from GSA's schedule for information technology equipment, software, and services.

4. **The Federal Cybersecurity Risk Determination Report and Action plan found that federal agencies lack awareness of, capacity to mitigate, and accountability for their cybersecurity. This report came out in 2017, 4 years after the CDM contract was put in place. Does GAO assess that GSA or DHS have measured the effectiveness of the CDM program, and if so, how?**

   We have not assessed whether or how GSA or DHS have measured the effectiveness of the CDM program. However, in May 2018, we reported that, at the direction of DHS leadership, the program had organized its previous 12 key performance parameters into 5 core security functions—identification, protection, detection, response, and recovery—to better align the performance parameters with the National Institute of Standards and Technology's Cybersecurity Framework.[6] As part of our planned work in response to the aforementioned request to examine agencies' continuous monitoring programs, we plan to identify and assess any performance metrics that GSA or DHS have developed to measure the effectiveness of the CDM program.

[5] GAO, Homeland Security Acquisitions: Leveraging Programs' Results Could Further DHS's Progress to Improve Portfolio Management, GAO-18-339SP (Washington, D.C.: May 2018).

[6] GAO-18-339SP.

5. **Can GAO explain the ultimate return on investment to the federal government from this centralized CDM program? Is CDM the appropriate solution, or would the U.S. government benefit more from outcome-based cybersecurity requirements for each federal agency?**

We have not determined the ultimate return on investment to the federal government from the centralized CDM program, nor have we determined if CDM is the appropriate solution, or if the government would benefit more from outcome-based cybersecurity requirements for each federal agency. However, in May 2018, we reported on the CDM program's new acquisition program baseline and cost, schedule, and performance parameters.[7] Among other things, our report noted the following:

- The operations and maintenance (O&M) cost thresholds for the CDM program had previously decreased by $1.2 billion, in part, because DHS leadership determined that the program would only fund CDM tools for the first 2 years after deployment; however, the O&M cost thresholds recently increased by $631 million when the program shifted some potential acquisition costs to be consistent with DHS's new appropriation structure, among other things.
- The acquisition costs for the program did not increase despite challenges with the phase 1 implementation, in part, because coverage for the U.S. Postal Service will no longer be funded by the CDM program.
- The program's full operational capability (FOC) date slipped by almost 4 years after the definition of FOC was revised (from meaning when the tools from CDM phases 1 through 3 are deployed at five agencies to being when the tools are available to all agencies participating in the CDM program). However, the program's costs could increase and its FOC date may slip further once the program establishes goals for phase 4. NPPD officials said they were unable to complete planning efforts for phase 4 in time to incorporate it into the most recent revision to the acquisition program baseline and, therefore, plan to re-baseline the CDM program again in 2018.

The CDM program identified a potential acquisition affordability gap in fiscal year 2018 based on its revised life-cycle cost estimate, which it addressed by adjusting the phase 3 schedule to shift some acquisition costs out to fiscal year 2020. However, the affordability gap from fiscal years 2018 to 2022 may be overstated because DHS's funding plan to Congress no longer contains O&M funding for individual programs. The program anticipates receiving approximately $281 million in O&M funding over the 5-year period.

6. **The 2017 Report to the President on Federal IT Modernization emphasizes a migration to cloud-based and shared services. What is GAO's assessment of the suitability of the current CDM program to these modernizations goals?**

We have not assessed the suitability of the current CDM program in relation to the modernizations goals of migrating to cloud-based and shared services. As part of our upcoming review of agencies continuous monitoring programs, we plan to assess how CDM supports agency actions for migrating to cloud-based and shared services.

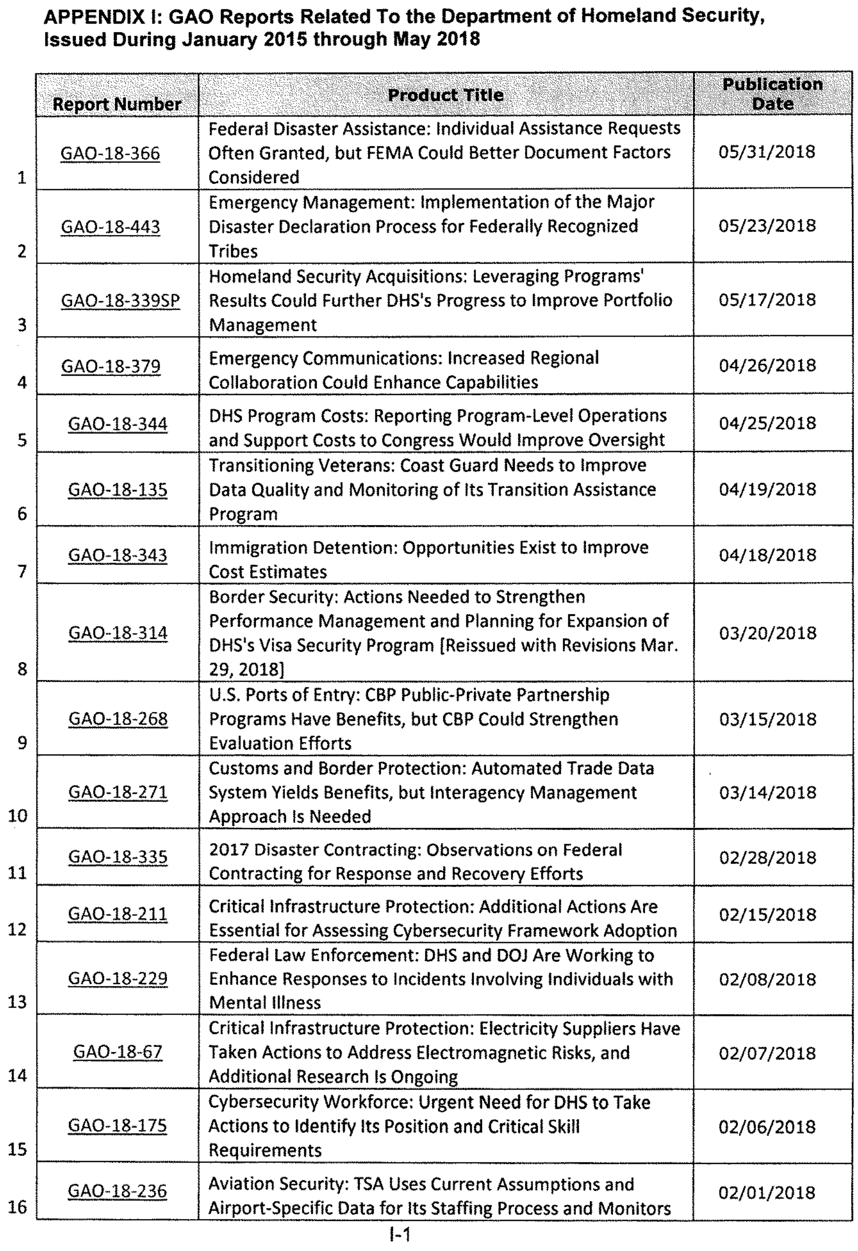
[7] GAO-18-339SP.

## Question for the Record from Senator Rand Paul
## Committee on Homeland Security and Governmental Affairs

1. **Mr. Rosenbach indicated reporting requirements may impress an excessive burden on DHS and GAO. Please provide for the record a list of reports GAO has been charged to complete relating to DHS, including all reports delivered over the last three years, reports not yet completed, and recurring reports to be delivered in the future.**

   Over the last 3 years (since January 2015), GAO has publicly released 211 reports that related to work at the Department of Homeland Security (DHS), including 7 that addressed cybersecurity-related issues. These reports are identified in appendix I.

   In addition, GAO currently has 133 ongoing engagements that are related to work at DHS, which include a number of engagements that have a government-wide scope. These engagements also include 10 that are planned to address cybersecurity-related issues. The ongoing engagements are identified in appendix II.



## APPENDIX I: GAO Reports Related To the Department of Homeland Security, Issued During January 2015 through May 2018

| | Report Number | Product Title | Publication Date |
|---|---|---|---|
| 1 | GAO-18-366 | Federal Disaster Assistance: Individual Assistance Requests Often Granted, but FEMA Could Better Document Factors Considered | 05/31/2018 |
| 2 | GAO-18-443 | Emergency Management: Implementation of the Major Disaster Declaration Process for Federally Recognized Tribes | 05/23/2018 |
| 3 | GAO-18-339SP | Homeland Security Acquisitions: Leveraging Programs' Results Could Further DHS's Progress to Improve Portfolio Management | 05/17/2018 |
| 4 | GAO-18-379 | Emergency Communications: Increased Regional Collaboration Could Enhance Capabilities | 04/26/2018 |
| 5 | GAO-18-344 | DHS Program Costs: Reporting Program-Level Operations and Support Costs to Congress Would Improve Oversight | 04/25/2018 |
| 6 | GAO-18-135 | Transitioning Veterans: Coast Guard Needs to Improve Data Quality and Monitoring of Its Transition Assistance Program | 04/19/2018 |
| 7 | GAO-18-343 | Immigration Detention: Opportunities Exist to Improve Cost Estimates | 04/18/2018 |
| 8 | GAO-18-314 | Border Security: Actions Needed to Strengthen Performance Management and Planning for Expansion of DHS's Visa Security Program [Reissued with Revisions Mar. 29, 2018] | 03/20/2018 |
| 9 | GAO-18-268 | U.S. Ports of Entry: CBP Public-Private Partnership Programs Have Benefits, but CBP Could Strengthen Evaluation Efforts | 03/15/2018 |
| 10 | GAO-18-271 | Customs and Border Protection: Automated Trade Data System Yields Benefits, but Interagency Management Approach Is Needed | 03/14/2018 |
| 11 | GAO-18-335 | 2017 Disaster Contracting: Observations on Federal Contracting for Response and Recovery Efforts | 02/28/2018 |
| 12 | GAO-18-211 | Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption | 02/15/2018 |
| 13 | GAO-18-229 | Federal Law Enforcement: DHS and DOJ Are Working to Enhance Responses to Incidents Involving Individuals with Mental Illness | 02/08/2018 |
| 14 | GAO-18-67 | Critical Infrastructure Protection: Electricity Suppliers Have Taken Actions to Address Electromagnetic Risks, and Additional Research Is Ongoing | 02/07/2018 |
| 15 | GAO-18-175 | Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements | 02/06/2018 |
| 16 | GAO-18-236 | Aviation Security: TSA Uses Current Assumptions and Airport-Specific Data for Its Staffing Process and Monitors | 02/01/2018 |

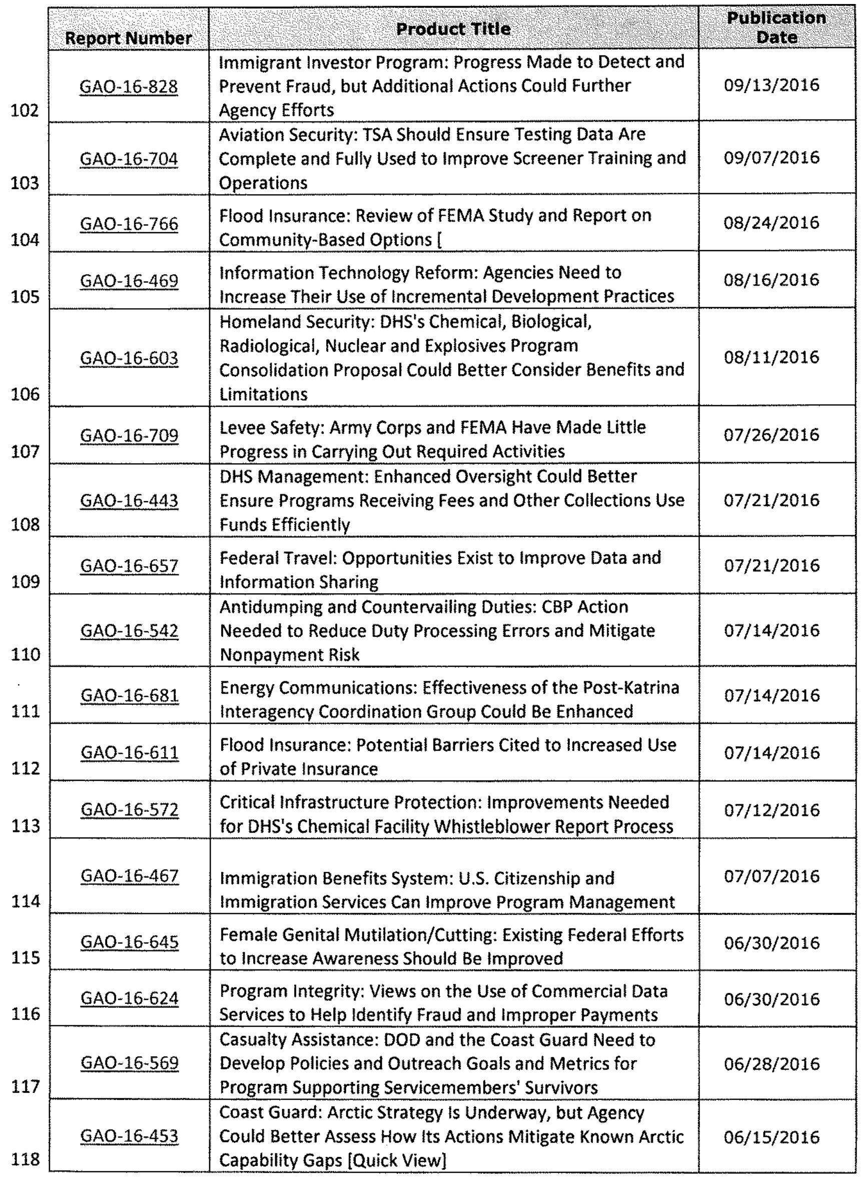
| | Report Number | Product Title | Publication Date |
|---|---|---|---|
| | | Passenger Wait Times Using Daily Operations Data | |
| 17 | GAO-18-252 | Next Generation 911: National 911 Program Could Strengthen Efforts to Assist States | 01/31/2018 |
| 18 | GAO-18-207 | Small Business Research Programs: Agencies Need to Take Steps to Assess Progress Toward Commercializing Technologies | 01/31/2018 |
| 19 | GAO-18-216 | Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market | 01/30/2018 |
| 20 | GAO-18-59 | Coast Guard Health Records: Timely Acquisition of New System Is Critical to Overcoming Challenges with Paper Process | 01/24/2018 |
| 21 | GAO-18-233 | Emergency Management: Federal Agencies Could Improve Dissemination of Resources to Colleges | 01/23/2018 |
| 22 | GAO-18-201 | VA Facility Security: Policy Review and Improved Oversight Strategy Needed | 01/11/2018 |
| 23 | GAO-18-214 | Nuclear Security: CBP Needs to Take Action to Ensure Imported Radiological Material Is Properly Licensed | 01/10/2018 |
| 24 | GAO-18-172 | Transportation Security Administration: After Oversight Lapses, Compliance with Policy Governing Special Authority Has Been Strengthened | 12/21/2017 |
| 25 | GAO-18-143 | Disaster Recovery: Additional Actions Would Improve Data Quality and Timeliness of FEMA's Public Assistance Appeals Processing | 12/15/2017 |
| 26 | GAO-18-16 | Commercial Fishing Vessels: More Information Needed to Improve Classification Implementation | 12/14/2017 |
| 27 | GAO-18-180 | Transportation Security Administration: Surface Transportation Inspector Activities Should Align More Closely With Identified Risks | 12/14/2017 |
| 28 | GAO-18-178 | Aviation Security: TSA Strengthened Foreign Airport Assessments and Air Carrier Inspections, but Could Improve Analysis to Better Address Deficiencies | 12/04/2017 |
| 29 | GAO-18-119 | Southwest Border Security: Border Patrol Is Deploying Surveillance Technologies but Needs to Improve Data Quality and Assess Effectiveness | 11/30/2017 |
| 30 | GAO-18-116 | Government Procurement: Effect of Restriction on DHS's Purchasing of Foreign Textiles Is Limited | 11/21/2017 |
| 31 | GAO-18-50 | Border Patrol: Issues Related to Agent Deployment Strategy and Immigration Checkpoints | 11/08/2017 |
| 32 | GAO-18-30 | Disaster Assistance: Opportunities to Enhance Implementation of the Redesigned Public Assistance Grant Program | 11/08/2017 |
| 33 | GAO-18-62 | Critical Infrastructure Protection: DHS Risk Assessments Inform Owner and Operator Protection Efforts and | 10/30/2017 |

| | Report Number | Product Title | Publication Date |
|---|---|---|---|
| | | Departmental Strategic Planning | |
| 34 | GAO-18-13 | Coast Guard: Actions Needed to Enhance Performance Information Transparency and Monitoring | 10/27/2017 |
| 35 | GAO-18-9 | Coast Guard: Actions Needed to Close Stations Identified as Overlapping and Unnecessarily Duplicative | 10/26/2017 |
| 36 | GAO-18-72 | Federal Facility Security: Selected Agencies Should Improve Methods for Assessing and Monitoring Risk | 10/26/2017 |
| 37 | GAO-18-46 | TSA Modernization: Use of Sound Program Management and Oversight Practices Is Needed to Avoid Repeating Past Problems | 10/17/2017 |
| 38 | GAO-18-10 | Counternarcotics: Overview of U.S. Efforts in the Western Hemisphere | 10/13/2017 |
| 39 | GAO-18-155 | Biodefense: Federal Efforts to Develop Biological Threat Awareness | 10/11/2017 |
| 40 | GAO-18-21 | Tobacco Trade: Duty-Free Cigarettes Sold in Unlimited Quantities on the U.S.-Mexico Border Pose Customs Challenges | 10/11/2017 |
| 41 | GAO-18-11 | Southwest Border Security: Actions Needed to Enhance CBP's Maintenance of Roads Used for Its Operations | 10/04/2017 |
| 42 | GAO-17-738 | Federal Contracting: Additional Management Attention and Action Needed to Close Contracts and Reduce Audit Backlog | 09/28/2017 |
| 43 | GAO-17-799 | DHS Financial Management: Better Use of Best Practices Could Help Manage System Modernization Project Risks | 09/26/2017 |
| 44 | GAO-17-559 | Drinking Water and Wastewater Infrastructure: Information on Identified Needs, Planning for Future Conditions, and Coordination of Project Funding | 09/20/2017 |
| 45 | GAO-17-629 | Coast Guard: Workforce Actions Under Way to Address Backlog in Recreational Vessel Documentation | 09/12/2017 |
| 46 | GAO-17-711 | Public Relations Spending: Selected Agencies' Activities Supported by Contracts and Public Affairs Staff | 09/12/2017 |
| 47 | GAO-17-794 | Aviation Security: Actions Needed to Systematically Evaluate Cost and Effectiveness Across Security Countermeasures | 09/11/2017 |
| 48 | GAO-17-662 | Aviation Security: TSA Has Made Progress Implementing Requirements in the Aviation Security Act of 2016 | 09/07/2017 |
| 49 | GAO-17-448 | Data Center Optimization: Agencies Need to Address Challenges and Improve Progress to Achieve Cost Savings Goal | 08/15/2017 |
| 50 | GAO-17-606 | International Mail Security: Costs and Benefits of Using Electronic Data to Screen Mail Need to Be Assessed | 08/02/2017 |

| | Report Number | Product Title | Publication Date |
|---|---|---|---|
| 51 | GAO-17-706 | Refugees: Actions Needed by State Department and DHS to Further Strengthen Applicant Screening Process and Assess Fraud Risks | 07/31/2017 |
| 52 | GAO-17-649 | Foreign Trade Zones: CBP Should Strengthen Its Ability to Assess and Respond to Compliance Risks across the Program | 07/27/2017 |
| 53 | GAO-17-650 | Supply Chain Security: CBP Needs to Enforce Compliance and Assess the Effectiveness of the Importer Security Filing and Additional Carrier Requirements | 07/20/2017 |
| 54 | GAO-17-687SP | Countering ISIS and Its Effects: Key Issues for Oversight | 07/18/2017 |
| 55 | GAO-17-613 | Federal Emergency Management Agency: Additional Actions Needed to Improve Handling of Employee Misconduct Allegations | 07/18/2017 |
| 56 | GAO-17-502 | Critical Infrastructure Protection: DHS Has Fully Implemented Its Chemical Security Expedited Approval Program, and Participation to Date Has Been Limited | 06/29/2017 |
| 57 | GAO-17-618 | Customs and Border Protection: Improved Planning Needed to Strengthen Trade Enforcement | 06/12/2017 |
| 58 | GAO-17-388 | Data Center Optimization: Agencies Need to Complete Plans to Address Inconsistencies in Reported Savings | 05/18/2017 |
| 59 | GAO-17-284 | Homeland Security: Progress Made to Implement IT Reform, but Additional Chief Information Officer Involvement Needed | 05/18/2017 |
| 60 | GAO-17-398 | Service Contracts: Agencies Should Take Steps to More Effectively Use Independent Government Cost Estimates | 05/17/2017 |
| 61 | GAO-17-474 | Border Security: Additional Actions Could Strengthen DHS Efforts to Address Subterranean, Aerial, and Maritime Smuggling | 05/01/2017 |
| 62 | GAO-17-425 | Flood Insurance: Comprehensive Reform Could Improve Solvency and Enhance Resilience | 04/27/2017 |
| 63 | GAO-17-426 | Federally Owned Vehicles: Agencies Should Improve Processes to Identify Underutilized Vehicles | 04/25/2017 |
| 64 | GAO-17-337 | Small Business Research Programs: Additional Actions Needed to Implement Fraud, Waste, and Abuse Prevention Requirements | 04/25/2017 |
| 65 | GAO-17-329 | Federal Contracts: Agencies Widely Used Indefinite Contracts to Provide Flexibility to Meet Mission Needs | 04/13/2017 |
| 66 | GAO-17-396 | Homeland Security Acquisitions: Identifying All Non-Major Acquisitions Would Advance Ongoing Efforts to Improve Management | 04/13/2017 |
| 67 | GAO-17-300 | Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts | 04/06/2017 |

| | Report Number | Product Title | Publication Date |
|---|---|---|---|
| 68 | GAO-17-346SP | Homeland Security Acquisitions: Earlier Requirements Definition and Clear Documentation of Key Decisions Could Facilitate Ongoing Progress | 04/06/2017 |
| 69 | GAO-17-325 | Human Trafficking: Action Needed to Identify the Number of Native American Victims Receiving Federally-funded Services | 03/30/2017 |
| 70 | GAO-17-470 | International Air Travelers: CBP Collaborates with Stakeholders to Facilitate the Arrivals Process, but Could Strengthen Reporting of Airport Wait Times | 03/30/2017 |
| 71 | GAO-17-202 | Maritime Environment: Federal and State Actions, Expenditures, and Challenges to Addressing Abandoned and Derelict Vessels | 03/28/2017 |
| 72 | GAO-17-204 | Immigration Status Verification for Benefits: Actions Needed to Improve Effectiveness and Oversight | 03/23/2017 |
| 73 | GAO-17-218 | Coast Guard Cutters: Depot Maintenance Is Affecting Operational Availability and Cost Estimates Should Reflect Actual Expenditures | 03/02/2017 |
| 74 | GAO-17-170 | Border Security: DHS Has Made Progress in Planning for a Biometric Air Exit System and Reporting Overstays, but Challenges Remain | 02/27/2017 |
| 75 | GAO-17-152 | Border Security: Additional Actions Needed to Strengthen Collection of Unmanned Aerial Systems and Aerostats Data | 02/16/2017 |
| 76 | GAO-17-215 | Federal Courthouses: Actions Needed to Enhance Capital Security Program and Improve Collaboration | 02/16/2017 |
| 77 | GAO-17-331 | Southwest Border Security: Additional Actions Needed to Better Assess Fencing's Contributions to Operations and Provide Guidance for Identifying Capability Gaps | 02/16/2017 |
| 78 | GAO-17-150 | Defense Civil Support: DOD, HHS, and DHS Should Use Existing Coordination Mechanisms to Improve Their Pandemic Preparedness | 02/10/2017 |
| 79 | GAO-17-84 | Supply Chain Security: Providing Guidance and Resolving Data Problems Could Improve Management of the Customs-Trade Partnership Against Terrorism Program | 02/08/2017 |
| 80 | GAO-17-182 | Critical Infrastructure Protection: Additional Actions by DHS Could Help Identify Opportunities to Harmonize Access Control Efforts | 02/07/2017 |
| 81 | GAO-17-200 | Federal Disaster Assistance: FEMA's Progress in Aiding Individuals with Disabilities Could Be Further Enhanced | 02/07/2017 |
| 82 | GAO-17-58 | Radioactive Sources: Opportunities Exist for Federal Agencies to Strengthen Transportation Security | 02/07/2017 |
| 83 | GAO-17-163 | Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely | 02/01/2017 |
| 84 | GAO-17-40 | Coast Guard: Most Training Providers Expect to Implement Revised International Maritime Standards by the Deadline Despite Challenges | 01/31/2017 |

| | Report Number | Product Title | Publication Date |
|---|---|---|---|
| 85 | GAO-17-114 | Military Personnel: DOD and the Coast Guard Need to Screen for Gambling Disorder Addiction and Update Guidance | 01/30/2017 |
| 86 | GAO-17-153 | Electricity: Federal Efforts to Enhance Grid Resilience | 01/25/2017 |
| 87 | GAO-17-216 | Border Security: CBP Aims to Prevent High-Risk Travelers from Boarding U.S.-Bound Flights, but Needs to Evaluate Program Performance | 01/24/2017 |
| 88 | GAO-17-66 | Border Patrol: Actions Needed to Improve Oversight of Post-Apprehension Consequences | 01/12/2017 |
| 89 | GAO-17-177 | Bioforensics: DHS Needs to Conduct a Formal Capability Gap Analysis to Better Identify and Address Gaps | 01/11/2017 |
| 90 | GAO-17-79 | Declining Resources: Selected Agencies Took Steps to Minimize Effects on Mission but Opportunities Exist for Additional Action | 12/20/2016 |
| 91 | GAO-17-123 | Federal Building Management: Building Disposal Authorities Provide Varying Degrees of Flexibility and Opportunities for Use | 12/08/2016 |
| 92 | GAO-17-36 | Flood Insurance: FEMA Needs to Address Data Quality and Consider Company Characteristics When Revising Its Compensation Methodology | 12/08/2016 |
| 93 | GAO-17-57 | Radiation Portal Monitors: DHS's Fleet Is Lasting Longer than Expected, and Future Acquisitions Focus on Operational Efficiencies | 10/31/2016 |
| 94 | GAO-17-171 | Homeland Security Acquisitions: Joint Requirements Council's Initial Approach Is Generally Sound and It Is Developing a Process to Inform Investment Priorities | 10/24/2016 |
| 95 | GAO-17-24 | Presidential Travel: Estimated Costs for a Specific Presidential Trip to Illinois and Florida | 10/11/2016 |
| 96 | GAO-17-12 | Emergency Communications: Improved Procurement of Land Mobile Radios Could Enhance Interoperability and Cut Costs | 10/05/2016 |
| 97 | GAO-16-511 | Information Technology: Agencies Need to Improve Their Application Inventories to Achieve Additional Savings | 09/29/2016 |
| 98 | GAO-16-717 | Combating Wildlife Trafficking: Agencies Are Taking a Range of Actions, but the Task Force Lacks Performance Targets for Assessing Progress | 09/22/2016 |
| 99 | GAO-16-797 | Federal Disaster Assistance: Federal Departments and Agencies Obligated at Least $277.6 Billion during Fiscal Years 2005 through 2014 | 09/22/2016 |
| 100 | GAO-16-744 | Fire Grants: FEMA Could Enhance Program Administration and Performance Assessment | 09/15/2016 |
| 101 | GAO-16-764 | Federal Air Marshal Service: Additional Actions Needed to Ensure Air Marshals' Mission Readiness | 09/14/2016 |



| | Report Number | Product Title | Publication Date |
|---|---|---|---|
| 102 | GAO-16-828 | Immigrant Investor Program: Progress Made to Detect and Prevent Fraud, but Additional Actions Could Further Agency Efforts | 09/13/2016 |
| 103 | GAO-16-704 | Aviation Security: TSA Should Ensure Testing Data Are Complete and Fully Used to Improve Screener Training and Operations | 09/07/2016 |
| 104 | GAO-16-766 | Flood Insurance: Review of FEMA Study and Report on Community-Based Options [ | 08/24/2016 |
| 105 | GAO-16-469 | Information Technology Reform: Agencies Need to Increase Their Use of Incremental Development Practices | 08/16/2016 |
| 106 | GAO-16-603 | Homeland Security: DHS's Chemical, Biological, Radiological, Nuclear and Explosives Program Consolidation Proposal Could Better Consider Benefits and Limitations | 08/11/2016 |
| 107 | GAO-16-709 | Levee Safety: Army Corps and FEMA Have Made Little Progress in Carrying Out Required Activities | 07/26/2016 |
| 108 | GAO-16-443 | DHS Management: Enhanced Oversight Could Better Ensure Programs Receiving Fees and Other Collections Use Funds Efficiently | 07/21/2016 |
| 109 | GAO-16-657 | Federal Travel: Opportunities Exist to Improve Data and Information Sharing | 07/21/2016 |
| 110 | GAO-16-542 | Antidumping and Countervailing Duties: CBP Action Needed to Reduce Duty Processing Errors and Mitigate Nonpayment Risk | 07/14/2016 |
| 111 | GAO-16-681 | Energy Communications: Effectiveness of the Post-Katrina Interagency Coordination Group Could Be Enhanced | 07/14/2016 |
| 112 | GAO-16-611 | Flood Insurance: Potential Barriers Cited to Increased Use of Private Insurance | 07/14/2016 |
| 113 | GAO-16-572 | Critical Infrastructure Protection: Improvements Needed for DHS's Chemical Facility Whistleblower Report Process | 07/12/2016 |
| 114 | GAO-16-467 | Immigration Benefits System: U.S. Citizenship and Immigration Services Can Improve Program Management | 07/07/2016 |
| 115 | GAO-16-645 | Female Genital Mutilation/Cutting: Existing Federal Efforts to Increase Awareness Should Be Improved | 06/30/2016 |
| 116 | GAO-16-624 | Program Integrity: Views on the Use of Commercial Data Services to Help Identify Fraud and Improper Payments | 06/30/2016 |
| 117 | GAO-16-569 | Casualty Assistance: DOD and the Coast Guard Need to Develop Policies and Outreach Goals and Metrics for Program Supporting Servicemembers' Survivors | 06/28/2016 |
| 118 | GAO-16-453 | Coast Guard: Arctic Strategy Is Underway, but Agency Could Better Assess How Its Actions Mitigate Known Arctic Capability Gaps [Quick View] | 06/15/2016 |

| | Report Number | Product Title | Publication Date |
|---|---|---|---|
| 119 | GAO-16-510 | Managing for Results: Agencies Need to Fully Identify and Report Major Management Challenges and Actions to Resolve them in their Agency Performance Plans | 06/15/2016 |
| 120 | GAO-16-494 | IT Dashboard: Agencies Need to Fully Consider Risks When Rating Their Major Investments | 06/02/2016 |
| 121 | GAO-16-632 | Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates | 05/31/2016 |
| 122 | GAO-16-582 | Federal Air Marshal Service: Actions Needed to Better Incorporate Risk in Deployment Strategy | 05/31/2016 |
| 123 | GAO-16-476 | Disaster Recovery: FEMA Needs to Assess Its Effectiveness in Implementing the National Disaster Recovery Framework | 05/26/2016 |
| 124 | GAO-16-514 | Immigration Detention: Additional Actions Needed to Strengthen DHS Management of Short-Term Holding Facilities | 05/26/2016 |
| 125 | GAO-16-468 | Information Technology: Federal Agencies Need to Address Aging Legacy Systems | 05/25/2016 |
| 126 | GAO-16-379 | Coast Guard: Actions Needed to Improve Strategic Allocation of Assets and Determine Workforce Requirements | 05/24/2016 |
| 127 | GAO-16-526 | Government Purchase Cards: Opportunities Exist to Leverage Buying Power | 05/19/2016 |
| 128 | GAO-16-498 | Visa Waiver Program: DHS Should Take Steps to Ensure Timeliness of Information Needed to Protect U.S. National Security | 05/05/2016 |
| 129 | GAO-16-371 | Quadrennial Homeland Security Review: Improved Risk Analysis and Stakeholder Consultations Could Enhance Future Reviews | 04/15/2016 |
| 130 | GAO-16-325 | Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance | 04/07/2016 |
| 131 | GAO-16-306 | Information Technology: FEMA Needs to Address Management Weaknesses to Improve Its Systems | 04/05/2016 |
| 132 | GAO-16-338SP | Homeland Security Acquisitions: DHS Has Strengthened Management, but Execution and Affordability Concerns Endure | 03/31/2016 |
| 133 | GAO-16-243 | Critical Infrastructure Protection: Federal Agencies Have Taken Actions to Address Electromagnetic Risks, but Opportunities Exist to Further Assess Risks and Strengthen Collaboration | 03/24/2016 |
| 134 | GAO-16-384 | Federal Protective Service: Enhancements to Performance Measures and Data Quality Processes Could Improve Human Capital Planning | 03/24/2016 |
| 135 | GAO-16-342 | Administrative Leave: Evaluation of DHS's New Policy Can Help Identify Progress toward Reducing Leave Use | 03/23/2016 |

| | Report Number | Product Title | Publication Date |
|---|---|---|---|
| 136 | GAO-16-305 | High-Containment Laboratories: Comprehensive and Up-to-Date Policies and Stronger Oversight Mechanisms Needed to Improve Safety | 03/21/2016 |
| 137 | GAO-16-59 | National Flood Insurance Program: Continued Progress Needed to Fully Address Prior GAO Recommendations on Rate-Setting Methods | 03/17/2016 |
| 138 | GAO-16-144 | Emergency Management: Improved Federal Coordination Could Better Assist K-12 Schools Prepare for Emergencies | 03/10/2016 |
| 139 | GAO-16-249 | Energy Communications: Actions Needed to Better Coordinate Federal Efforts in the National Capital Region | 03/10/2016 |
| 140 | GAO-16-323 | Data Center Consolidation: Agencies Making Progress, but Planned Savings Goals Need to Be Established | 03/03/2016 |
| 141 | GAO-16-71 | Navy and Coast Guard Shipbuilding: Navy Should Reconsider Approach to Warranties for Correcting Construction Defects | 03/03/2016 |
| 142 | GAO-16-231 | Immigration Detention: Additional Actions Needed to Strengthen Management and Oversight of Detainee Medical Care | 02/29/2016 |
| 143 | GAO-16-176 | Transportation Security: Status of GAO Recommendations on TSA's Security-Related Technology Acquisitions | 02/17/2016 |
| 144 | GAO-16-285 | Transportation Security: TSA Has Taken Actions to Address Transportation Security Acquisition Reform Act Requirements | 02/17/2016 |
| 145 | GAO-16-236 | Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk | 02/16/2016 |
| 146 | GAO-16-253 | Homeland Security: Oversight of Neglected Human Resources Information Technology Investment Is Needed | 02/11/2016 |
| 147 | GAO-16-190 | National Flood Insurance Program: Options for Providing Affordability Assistance | 02/10/2016 |
| 148 | GAO-16-288 | U.S. Secret Service: Data Analyses Could Better Inform the Domestic Field Office Structure | 02/10/2016 |
| 149 | GAO-16-226 | DOD and Coast Guard: Actions Needed to Increase Oversight and Management Information on Hazing Incidents Involving Servicemembers | 02/09/2016 |
| 150 | GAO-16-87 | Disaster Response: FEMA Has Made Progress Implementing Key Programs, but Opportunities for Improvement Exist | 02/05/2016 |
| 151 | GAO-16-38 | Federal Emergency Management Agency: Strengthening Regional Coordination Could Enhance Preparedness Efforts | 02/04/2016 |
| 152 | GAO-16-294 | Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System | 01/28/2016 |
| 153 | GAO-16-274 | U.S. Border Communities: Ongoing DOT Efforts Could Help Address Impacts of International Freight Rail | 01/28/2016 |

| | Report Number | Product Title | Publication Date |
|---|---|---|---|
| 154 | GAO-16-148 | National Security Cutter: Enhanced Oversight Needed to Ensure Problems Discovered during Testing and Operations Are Addressed | 01/12/2016 |
| 155 | GAO-16-223 | Firearms Trafficking: U.S. Efforts to Combat Firearms Trafficking to Mexico Have Improved, but Some Collaboration Challenges Remain | 01/11/2016 |
| 156 | GAO-16-209 | Federal Acquisitions: Use of 'Other Transaction' Agreements Limited and Mostly for Research and Development Activities | 01/07/2016 |
| 157 | GAO-16-117 | TSA Acquisitions: Further Actions Needed to Improve Efficiency of Screening Technology Test and Evaluation | 12/17/2015 |
| 158 | GAO-16-127 | Air Travel and Communicable Diseases: Comprehensive Federal Plan Needed for U.S. Aviation System's Preparedness | 12/16/2015 |
| 159 | GAO-16-135 | Homeland Security: FPS and GSA Should Strengthen Collaboration to Enhance Facility Security | 12/16/2015 |
| 160 | GAO-16-167 | Internet Protocol Transition: FCC Should Strengthen Its Data Collection Efforts to Assess the Transition's Effects | 12/16/2015 |
| 161 | GAO-16-104 | Maritime Transportation: Implications of Using U.S. Liquefied-Natural-Gas Carriers for Exports | 12/03/2015 |
| 162 | GAO-16-50 | Asylum: Additional Actions Needed to Assess and Address Fraud Risks | 12/02/2015 |
| 163 | GAO-16-79 | Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress | 11/19/2015 |
| 164 | GAO-16-57 | National Security Personnel: Committed Leadership Is Needed for Implementation of Interagency Rotation Program | 11/17/2015 |
| 165 | GAO-16-19 | Screening Partnership Program: TSA Can Benefit from Improved Cost Estimates | 11/16/2015 |
| 166 | GAO-16-55 | Military Personnel: Oversight Framework and Evaluations Needed for DOD and the Coast Guard to Help Increase the Number of Female Officer Applicants | 11/13/2015 |
| 167 | GAO-16-10 | Electronic Monitoring: Draft National Standard for Offender Tracking Systems Addresses Common Stakeholder Needs | 10/26/2015 |
| 168 | GAO-16-99 | Biosurveillance: DHS Should Not Pursue BioWatch Upgrades or Enhancements Until System Capabilities Are Established | 10/23/2015 |
| 169 | GAO-15-783 | Disaster Contracting: FEMA Needs to Cohesively Manage Its Workforce and Fully Address Post-Katrina Reforms | 09/29/2015 |
| 170 | GAO-15-714 | Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs | 09/29/2015 |
| 171 | GAO-15-793 | Biosurveillance: Challenges and Options for the National Biosurveillance Integration Center | 09/24/2015 |

| | Report Number | Product Title | Publication Date |
|---|---|---|---|
| 172 | GAO-15-549 | Strategic Sourcing: Opportunities Exist to Better Manage Information Technology Services Spending | 09/22/2015 |
| 173 | GAO-15-733 | Child Welfare: Steps Have Been Taken to Address Unregulated Custody Transfers of Adopted Children | 09/16/2015 |
| 174 | GAO-15-718 | Federal User Fees: Key Considerations for Designing and Implementing Regulatory Fees | 09/16/2015 |
| 175 | GAO-15-807 | Confidential Informants: Updates to Policy and Additional Guidance Would Improve Oversight by DOJ and DHS Agencies | 09/15/2015 |
| 176 | GAO-15-617 | Information Technology Reform: Billions of Dollars in Savings Have Been Realized, but Agencies Need to Complete Reinvestment Plans | 09/15/2015 |
| 177 | GAO-15-682 | U.S. Coast Guard National Pollution Funds Center: Improved Controls Needed for Oil Removal Disbursements and Action Needed for Sustainable Funding | 09/15/2015 |
| 178 | GAO-15-781 | Emergency Management: FEMA Collaborates Effectively with Logistics Partners but Could Strengthen Implementation of Its Capabilities Assessment Tool | 09/10/2015 |
| 179 | GAO-15-788 | Managing for Results: Greater Transparency Needed in Public Reporting on the Quality of Performance Information for Selected Agencies' Priority Goals | 09/10/2015 |
| 180 | GAO-15-642 | Internet Management: Structured Evaluation Could Help Assess Proposed Transition of Key Domain Name and Other Technical Functions | 08/19/2015 |
| 181 | GAO-15-696 | Immigrant Investor Program: Additional Actions Needed to Better Assess Fraud Risks and Report Economic Benefits | 08/12/2015 |
| 182 | GAO-15-707 | Central America: Improved Evaluation Efforts Could Enhance Agency Programs to Reduce Unaccompanied Child Migration | 07/29/2015 |
| 183 | GAO-15-602 | Managing for Results: Practices for Effective Agency Strategic Reviews | 07/29/2015 |
| 184 | GAO-15-614 | Critical Infrastructure Protection: DHS Action Needed to Verify Some Chemical Facility Information and Manage Compliance Process | 07/22/2015 |
| 185 | GAO-15-521 | Unaccompanied Alien Children: Actions Needed to Ensure Children Receive Required Care in DHS Custody | 07/14/2015 |
| 186 | GAO-15-437 | Federal Emergency Management Agency: Additional Planning and Data Collection Could Help Improve Workforce Management Efforts | 07/09/2015 |
| 187 | GAO-15-579 | Managing for Results: Agencies Report Positive Effects of Data-Driven Reviews on Performance but Some Should Strengthen Practices | 07/07/2015 |
| 188 | GAO-15-509 | Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information | 07/02/2015 |

| | Report Number | Product Title | Publication Date |
|---|---|---|---|
| 189 | GAO-15-551 | DHS IT Contracting: Steps Taken to Enhance EAGLE II Small Business Opportunities, but Better Assessment Data Needed | 06/24/2015 |
| 190 | GAO-15-431 | Telecommunications: Agencies Need Better Controls to Achieve Significant Savings on Mobile Devices and Services | 05/21/2015 |
| 191 | GAO-15-415 | Immigration Benefits System: Better Informed Decision Making Needed on Transformation Program | 05/18/2015 |
| 192 | GAO-15-399 | Southwest Border: Issues Related to Private Property Damage | 04/30/2015 |
| 193 | GAO-15-171SP | Homeland Security Acquisitions: Major Program Assessments Reveal Actions Needed to Improve Accountability | 04/22/2015 |
| 194 | GAO-15-296 | Information Technology: Additional OMB and Agency Actions Needed to Ensure Portfolio Savings Are Realized and Effectively Tracked | 04/16/2015 |
| 195 | GAO-15-358 | Small Business Research Programs: Challenges Remain in Meeting Spending and Reporting Requirements | 04/15/2015 |
| 196 | GAO-15-271 | Federal Protective Service: More Effective Management Needed in Delegating Security Authority to Agencies | 03/31/2015 |
| 197 | GAO-15-445 | Homeland Security: Actions Needed to Better Manage Security Screening at Federal Buildings and Courthouses | 03/31/2015 |
| 198 | GAO-15-325 | Coast Guard Aircraft: Transfer of Fixed-Wing C-27J Aircraft Is Complex and Further Fleet Purchases Should Coincide with Study Results | 03/26/2015 |
| 199 | GAO-15-444 | Homeland Security: Action Needed to Better Assess Cost-Effectiveness of Security Enhancements at Federal Facilities | 03/24/2015 |
| 200 | GAO-15-201 | Border Security: Additional Efforts Needed to Address Persistent Challenges in Achieving Radio Interoperability | 03/23/2015 |
| 201 | GAO-15-222 | Municipalities in Fiscal Crisis: Federal Agencies Monitored Grants and Assisted Grantees, but More Could Be Done to Share Lessons Learned | 03/20/2015 |
| 202 | GAO-15-292 | Homeland Security Acquisitions: DHS Should Better Define Oversight Roles and Improve Program Reporting to Congress | 03/12/2015 |
| 203 | GAO-15-195 | Coast Guard: Timely Actions Needed to Address Risks in Using Rotational Crews | 03/06/2015 |
| 204 | GAO-15-263 | Combat Nuclear Smuggling: DHS Research and Development on Radiation Detection Technology Could Be Strengthened | 03/06/2015 |
| 205 | GAO-15-154 | H-2A and H-2B Visa Programs: Increased Protections Needed for Foreign Workers | 03/06/2015 |
| 206 | GAO-15-362 | Central America: Information on Migration of Unaccompanied Children from El Salvador Guatemala and | 02/27/2015 |

| | Report Number | Product Title | Publication Date |
|---|---|---|---|
| | | Honduras | |
| 207 | GAO-15-178 | Flood Insurance: Status of FEMA's Implementation of the Biggert-Waters Act, as Amended | 02/19/2015 |
| 208 | GAO-15-193 | Geospatial Data: Progress Needed on Identifying Expenditures, Building and Utilizing a Data Infrastructure, and Reducing Duplicative Efforts | 02/12/2015 |
| 209 | GAO-15-288 | Critical Technologies: Agency Initiatives Address Some Weaknesses, but Additional Interagency Collaboration Is Needed | 02/10/2015 |
| 210 | GAO-15-261 | Aviation Security: TSA Should Take Additional Action to Obtain Stakeholder Input when Modifying the Prohibited Items List | 02/04/2015 |
| 211 | GAO-15-294 | Supply Chain Security: CBP Needs to Enhance Its Guidance and Oversight of High-Risk Maritime Cargo Shipments | 01/27/2015 |

**APPENDIX II: Ongoing GAO Engagements Related to Work at the Department of Homeland Security As of June 1, 2018**

| | Job Code | Engagement Topic | Programming Team |
|---|---|---|---|
| 1 | 100774 | Backdoor Authority Accounts | SI |
| 2 | 100782 | Federal Agile Software Guide | ARM |
| 3 | 101056 | Agency Chief Information Officer Authorities | IT |
| 4 | 101021 | Criminal Alien Statistics | HSJ |
| 5 | 101100 | National Security Checks for Refugee Applicants | HSJ |
| 6 | 101181 | Tribal Disaster Declarations | HSJ |
| 7 | 101189 | Federal Research for Transformational Technological Advances | NRE |
| 8 | 101196 | Puget Sound Restoration Efforts | NRE |
| 9 | 101198 | Federal Cybersecurity Workforce Assessment | IT |
| 10 | 101214 | Nonimmigrant Visa Security | HSJ |
| 11 | 101221 | FedRAMP Implementation | IT |
| 12 | 101241 | DHS Offices of Professional Responsibility | HSJ |
| 13 | 101290 | Native American Cultural Property: Agencies Could Better Collaborate to Assist Tribes in Facilitating the Return of Items from Overseas Auctions | NRE |
| 14 | 101295 | Regional Emergency Communications Assistance | PI |
| 15 | 101411 | Freedom of Information Act Compliance | IT |
| 16 | 101428 | Reverse Auctions | CNSA |
| 17 | 101430 | TSA Covert Testing | HSJ |
| 18 | 101431 | Threat of Chemical Terrorism | HSJ |
| 19 | 101433 | Tribal Consultation Practices | NRE |

| | Job Code | Engagement Topic | Programming Team |
|---|---|---|---|
| 20 | 101441 | FEMA's Individual Assistance Factors | HSJ |
| 21 | 101443 | DOD Authority on Committee on Foreign Investment in the U.S. (CFIUS) | CNSA |
| 22 | 101457 | TSA Cuba Airport Security | HSJ |
| 23 | 101695 | Contractors and Tax Debt | FAIS |
| 24 | 101937 | Coast Guard Recapitalization | CNSA |
| 25 | 101940 | 2018 DHS Major Acquisition Program Assessments | CNSA |
| 26 | 101966 | Presidential Security | DCM |
| 27 | 101985 | Animal Welfare in Federal Research | NRE |
| 28 | 101986 | Presidential Travel Costs | DCM |
| 29 | 102017 | U.S. Secret Service Campaign Travel Costs | HSJ |
| 30 | 102023 | Observations on DHS's CFATS Program | HSJ |
| 31 | 102032 | Noncompetitive and Bridge Contracts for Information Technology | CNSA |
| 32 | 102037 | North American Energy Integration | IAT |
| 33 | 102051 | USDA's Preparedness for Foot-and-Mouth Disease Outbreak | NRE |
| 34 | 102059 | Student and Exchange Visitor Program (SEVP) | FAIS |
| 35 | 102070 | DHS Requirements Process for Major Acquisitions | CNSA |
| 36 | 102091 | Immigration Detention Resource Requirements | HSJ |
| 37 | 102096 | Secret Service's IT Portfolio and Workforce | IT |
| 38 | 102116 | Pipeline Physical Security and Cybersecurity | HSJ |
| 39 | 102139 | Inventory Controls and Purchases of Firearms, Ammunition, and Tactical Equipment at Federal Agencies | HSJ |

| | Job Code | Engagement Topic | Programming Team |
|---|---|---|---|
| 40 | 102148 | Mariana Islands Workforce Data | IAT |
| 41 | 102150 | Federal Protective Service Organizational Benefits and Challenges | PI |
| 42 | 102153 | Air Cargo Security | HSJ |
| 43 | 102167 | Chemical Facility Security Issues | HSJ |
| 44 | 102189 | Federal Facility Emerging Threats | PI |
| 45 | 102190 | DHS Office of Strategy, Policy, and Plans | HSJ |
| 46 | 102197 | Foreign Trade Zones Board's Application Process | IAT |
| 47 | 102207 | Offshore Oil Spill Prevention, Response, and Restoration Efforts | NRE |
| 48 | 102221 | Emerging Threats of High National Security Consequence | DCM |
| 49 | 102230 | Coast Guard Icebreakers Acquisition | CNSA |
| 50 | 102243 | Promoting Effective Asset Management | PI |
| 51 | 102246 | U.S. Customs and Border Protection Recruitment and Hiring | HSJ |
| 52 | 102276 | Nonimmigrant Visa Screening and Vetting | HSJ |
| 53 | 102288 | TSA Passenger Screening Mechanisms to Prevent Profiling | HSJ |
| 54 | 102297 | FEMA's Homeland Security Grants Program Awards and Management Processes | HSJ |
| 55 | 102299 | IT Cloud Computing | IT |
| 56 | 102323 | U.S. Counternarcotics Assistance to Colombia | IAT |
| 57 | 102336 | Southwest Border Wall | HSJ |
| 58 | 102341 | Federal Response to 2017 Hurricanes and Wildfires | HSJ |

| | Job Code | Engagement Topic | Programming Team |
|---|---|---|---|
| 59 | 102350 | Agency Use of Performance Information Index | SI |
| 60 | 102356 | TSA Acquisition Improvements | HSJ |
| 61 | 102362 | Integration of Physical Access Control Systems | PI |
| 62 | 102370 | Northern Border Security | HSJ |
| 63 | 102374 | Executive Orders on Border Security and Immigration | HSJ |
| 64 | 102385 | Aviation Security: Transportation Security Officer Basic Training at the Federal Law Enforcement Training Center | HSJ |
| 65 | 102388 | FEMA Government Continuity Programs | HSJ |
| 66 | 102389 | Electronic Delivery of Social Security Numbers Testimony | EWIS |
| 67 | 102392 | U.S. Efforts to Train Central American Police | IAT |
| 68 | 102398 | Effectiveness of NRC Security Requirements for Radiological Material | NRE |
| 69 | 102403 | DHS Research and Development Spending and Oversight | HSJ |
| 70 | 102408 | Coast Guard Shore Infrastructure | HSJ |
| 71 | 102410 | Buy American Act | CNSA |
| 72 | 102414 | FY 2018 Key Issues Update | SI |
| 73 | 102425 | FDA Import Alerts for Seafood | NRE |
| 74 | 102427 | Immigration Enforcement Priorities | HSJ |
| 75 | 102431 | U.S. Efforts to Support Reintegration of Central American Migrants | IAT |
| 76 | 102432 | Federal Efforts in Environmental Justice | NRE |
| 77 | 102437 | Secret Service Dual Mission | HSJ |

| | Job Code | Engagement Topic | Programming Team |
|---|---|---|---|
| 78 | 102451 | Access to Federally Funded Research and Data | NRE |
| 79 | 102454 | Employment Identity Theft Fraud | SI |
| 80 | 102464 | Federal Reliance on Credit Reporting Agencies | IT |
| 81 | 102466 | DHS's Securing the Cities Program | NRE |
| 82 | 102473 | Visa Security Program | HSJ |
| 83 | 102476 | Agency Compliance with the Improper Payments Elimination and Recovery Act (IPERA) in Fiscal Years 2017 and 2016 | FMA |
| 84 | 102488 | DHS Interoperable Emergency Communication Efforts | PI |
| 85 | 102490 | Fed Intrusion Detection and Prevention Capabilities | IT |
| 86 | 102492 | U.S. Assistance to Central America | IAT |
| 87 | 102495 | FEMA Grants Management Modernization Program | IT |
| 88 | 102504 | DHS Agile Adoption | IT |
| 89 | 102509 | Federal Efforts to Address Antibiotic Resistance | ARM |
| 90 | 102528 | Committee on Foreign Investment in the United States: Real Estate Transactions | IAT |
| 91 | 102530 | Polar Icebreakers Acquisition | CNSA |
| 92 | 102556 | CBP Inspections at Land Ports of Entry | HSJ |
| 93 | 102559 | DHS Resolution of EEO Barriers | SI |
| 94 | 102566 | FITARA Best Practices | IT |
| 95 | 102585 | Electric Grid Cybersecurity | NRE |
| 96 | 102588 | Federal IT Workforce Planning | IT |
| 97 | 102589 | Benefit Programs for Servicemembers | EWIS |

| | Job Code | Engagement Topic | Programming Team |
|---|---|---|---|
| 98 | 102591 | Modernization of Federal Legacy Systems | IT |
| 99 | 102594 | Federal Cybersecurity Workforce Coding | IT |
| 100 | 102598 | DHS High Risk Area Monitoring | HSJ |
| 101 | 102600 | Export Controls of Firearms | IAT |
| 102 | 102609 | Puerto Rico Electricity Grid Restoration and Resilience | NRE |
| 103 | 102614 | Mission Critical IT Acquisitions | IT |
| 104 | 102621 | Bank Secrecy Act Implementation | FMCI |
| 105 | 102624 | Cybersecurity High-Risk Update | IT |
| 106 | 102626 | Removal of PII from Cyber Threat Indicators | IT |
| 107 | 102633 | Cybersecurity Risk Management | IT |
| 108 | 102654 | U.S. Virgin Islands and Puerto Rico Disaster Recovery Plans | HSJ |
| 109 | 102659 | Post-Disaster Contract Awards | CNSA |
| 110 | 102660 | Advance Disaster Contracts | CNSA |
| 111 | 102664 | FY 2018 Consolidated Financial Statement Audit of the U.S. Government | FMA |
| 112 | 102665 | CBP Infrastructure at Land Ports of Entry | HSJ |
| 113 | 102676 | FY18 Processes Used to Prepare the CFS of the U.S. Government | FMA |
| 114 | 102677 | Transportation Security Administration Cuba Airport Security | HSJ |
| 115 | 102683 | Equifax Breach | IT |
| 116 | 102691 | Intelligence Community Classification System | DCM |
| 117 | 102692 | 2018 Statement of Long-Term Fiscal Projections Audit | FMA |

| | Job Code | Engagement Topic | Programming Team |
|---|---|---|---|
| 118 | 102714 | Disaster Assistance for Older Americans and Individuals with Disabilities | EWIS |
| 119 | 102724 | DHS Border Security Metrics | HSJ |
| 120 | 102725 | TSA Passenger and Checked Baggage Screening Technologies | HSJ |
| 121 | 102743 | Data Center Optimization Progress and Practices | IT |
| 122 | 102748 | DHS Test and Evaluation | CNSA |
| 123 | 102751 | Federal Emergency Management Agency: Progress and Continuing Challenges in National Preparedness Efforts (Testimony) | HSJ |
| 124 | 102759 | Federal Response to the 2017 Western Wildfires | HSJ |
| 125 | 102770 | 2019 DHS Major Acquisition Program Assessments | CNSA |
| 126 | 102790 | Surface Transportation Research & Development | HSJ |
| 127 | 102795 | TSA Security Checkpoint Wait Times (Testimony) | HSJ |
| 128 | 102797 | Nonimmigrant Visa Adjudication and Response to 2017-18 Executive Actions | HSJ |
| 129 | 102800 | Secret Service Protective Mission Panel | HSJ |
| 130 | 102810 | DOJ Prioritization of Immigration-Only Offenses | HSJ |
| 131 | 102816 | Joint Interagency Task Forces | HSJ |
| 132 | 102818 | Mass Care after Disasters | EWIS |
| 133 | 102823 | Southwest Border Wall (Public Report) | HSJ |

**Post-Hearing Questions for the Record**
**Submitted to the Honorable Eric Rosenbach**
**From Senator Rand Paul**

**"Mitigating America's Cybersecurity Risk"**

**April 24, 2018**

1. Nearly all Americans protect their private and commercial communications with encryption tools like Virtual Private Networks (VPN) and Transport Layer Security (TLS). A number of governments have deliberately compromised the integrity of popular encryption tools. Of course, a flaw designed to make encryption more tractable by one government may be exploited by another.
   - Do flaws impacting the confidentiality of popular encryption tools represent a national security threat?
     **Strong encryption is an important part the United States economic and national security. Whenever possible, the U.S. should protect the integrity and confidentiality of encryption tools and algorithms.**

2. Some government officials seek to weaken the confidentiality of popular cryptography systems. These so-called "responsible encryption" proposals are variations of key escrow systems, where affected encrypted channels would be accessible by third parties.
   - Are key escrow systems appropriate for widespread military, government, or political campaign use?
   - Would compromise of a key escrow system used to access American cell phones, private messages, or other widespread technology represent a national security threat?
     **Key escrow systems are not appropriate for widespread military, government or campaign use. Yes, compromise of a key escrow system would represent a significant threat to the integrity of important to traditional telecommunications systems and emerging application-based communications.**

3. Under the *Federal Information Security Modernization Act of 2014*, DHS can compel executive branch departments and agencies to comply with Binding Operational Directives (BOD). Since 2014, only six BODs have been issued.
   - What issues should DHS consider for new BODs to reduce our national cybersecurity risk?
     **At the current time, DHS does not need to issue additional BODs. Rather than issuing new regulations, DHS and the federal government should focus on successfully implementing the numerous existing laws and regulations designed to improve cybersecurity.**

4. The Supreme Court established a border search exception to the Fourth Amendment, reasoning that the government has a special interest in physical containers at points of

entry because contraband must be physically introduced. Computing technology has had an immeasurable impact on the transport of information. By contrast, electronic contraband can be instantly transmitted across the planet. Mobile devices, free Wi-Fi, and special software obscure transmission sources and destinations, and content is protected by robust, ubiquitous protocols. This renders physical transport across a border to be the most expensive, most attributable, and slowest method available to smuggle digital contraband such as stolen intellectual property or "cyber weapons."

- What properties distinguish physical contraband from digital contraband?
- Does digital content on a device in Brownsville, Texas, pose a special threat not present with digital content on a device in Brownsville, Kentucky?

**Physical contraband may include items that pose a threat to national security because of kinetic effects, such as illegal weapons, including, potentially, a weapon that could kill thousands of Americans. The United States should dedicate additional resources to slowing the spread of destructive malware by designing and supporting modern non-proliferation regimes. That said, the US government currently supports some forms of export control that will significantly damage the US cybersecurity industry if fully implemented without amendments.**

**My genuine apologies, but without knowing additional facts about the hypothetical case of digital content in the two Brownsvilles I am unable to answer that specific question.**

**Post-Hearing Questions for the Record**
**Submitted to the Honorable Eric Rosenbach**
**From Senator Claire McCaskill**

**"Mitigating America's Cybersecurity Risk"**

**April 24, 2018**

Working with states

1. You and your colleagues at the Belfer Center have been working with states throughout the country conducting tabletop exercises and other events to help enhance election cybersecurity and planning. Given your exposure, how would you assess the status of our preparedness as a country for the upcoming elections?

   During our interaction with the states we have found that they take this issue very seriously, yet sometimes lack the resources and expertise to address all areas of risk. On the strategic level, social media platforms remain vulnerable to the same kind of exploitation by foreign information operations that we witnessed in 2016. The social media platforms continue to under deliver on promises that they make to improve the security, privacy and trustworthiness of their platforms. The nature of the threat has not changed, and we cannot afford complacency; cybersecurity preparations remain an urgent priority. Levels of completed preparations vary by state, but we have not yet achieved the "whole of nation" approach that is necessary to successfully mitigate the cyber threat to our election systems, regardless of increased public discourse over the last eighteen months, congressional funding, and ongoing state and federal coordination to address vulnerabilities.

2. Given your experience working with a variety of states that have varying levels of cyber sophistication and aging infrastructure, what are your biggest concerns regarding the upcoming midterm and 2020 elections and what suggestions do you have to address those?

   My primary concerns are the size of the attack surface, the challenges of achieving effective collaboration between state and federal actors, the absence of incident response strategies, and an emerging White House leadership void in cybersecurity. States with a decisive role in national elections face the most risk, yet it is difficult to be certain which will be targeted. Bad actors need only one success to undermine trust and confidence in the system, while we must successfully defend hundreds of points of vulnerability simultaneously and repeatedly. The states have voiced concerns about federal overreach in the election processes, which threatens to undermine the kind of effective collaboration that must be inherent to combating the cyber threat. In our work with the states who participated in Defending Digital Democracy's (D3P) 2018 tabletop exercises, we found that crisis communication and public affairs were often more difficult for officials than the technological aspect of security. Because Russia aimed to undermine trust in officials and processes by hacking the elections, it is vital that we incorporate understanding of that goal into our approach to the midterms and 2020 election.

Congress can address these concerns by committing to sustained and reliable funding for election cybersecurity efforts beyond the near-term $380 million authorized in the omnibus bill. The states need confidence in future federal budgetary support in order to fully commit to undertaking costly long-term responses and patching efforts. Addressing budgetary questions will help the federal government remain sensitive to state concerns and balance the need for accountability with the maintenance of a trusting partnership.

3. Do you think states understand the nature of the threat and are adequately preparing?

   Yes, D3P's engagement with the states showed that they understand the threat and have undertaken serious preparation to address vulnerabilities. However, on its own, a state does not have the resources to defend against a cyberattack of significant consequence. Resource limitations constrain their coordination of strategies, capabilities, and workforce. Since individuals and private sector organizations are also likely targets for future information operations, the states bear responsibility for improving their citizens' understanding of the nature of this threat as well.

Sanctions

1. Are sanctions against Russia changing Russia's behavior? If so, in what ways?

   Sanctions against Russia have likely fallen short of their desired effect because of the magnitude of Russia's success in 2016 and the lack of a cohesive American deterrence posture. The initial December 2016 sanctions were long overdue and had negligible impact on Russia's behavior: intelligence officials confirmed in congressional testimony earlier this year that Moscow still intended at the time to continue its cyber and information operations in the 2018 mid-term elections. It is too early to tell if the new tranche of sanctions imposed in April by the White House will change Russia's behavior in the long term, yet the incoherence of our national cybersecurity posture all but guarantees future attacks.

2. If current sanctions are not working, do you think a more robust sanctions regime would be effective against Russia, or are other tools needed to truly change Russia's behavior and deter it from interfering in our elections and those of our partners and allies?

   Sanctions alone do not impose sufficient costs on Russia to change its behavior unless they are paired with a strong declaratory policy that guarantees retaliation. We need a broader and more creative set of tools to raise the costs of Russian aggression while reducing the benefits the Kremlin perceives it can achieve. Such tools could include a commitment to immediate public attribution upon attempted interference (since attribution capabilities have improved dramatically in recent years), making the current sanctions regime longer and more robust, and visibly leading international capacity building efforts to protect election systems and disrupt malware proliferation. In the event of a cyberattack on our partners and allies, this demonstrates willingness to impose consequences. International collaboration is directly in our interests because allowing Russia to test their methods on other countries sans repercussions increases their ability to deploy refined malware against us.

3. What else do you think the United States should be doing to proactively stop Russia from interfering in U.S. elections?

   To recalibrate Russian perceptions and discourage future Russian interference, the United States should adopt a three-pronged strategy: bolstering domestic defensive capabilities to deny opportunities for attack, sharpening legal offensive capabilities to disrupt any attacks at their source, and adopting a public deterrence posture that raises the costs of cyberattacks while diminishing their benefits. We need to establish our willingness to act in order to guarantee costs and consequences for attempted interference. The DHS decision to designate election systems as critical infrastructure was an important foundation for future efforts, since it sends a strong message to the Russians and any other tempted adversary that the costs of attacking these systems are higher than they may have been before. Moreover, we need to commit to a stronger declaratory policy, leveraging improvements in our attribution capabilities to reassure the world that we will attribute attacks to their source immediately following detection so that adversaries cannot continue to hide in the shadows.

   The federal government must also force online platforms like Facebook and Twitter to mitigate the effects of future hostile information operations and prevent to the greatest extent possible their exploitation in such operations. Their efforts to date have been scattered, weak and primarily focused on improving their press coverage.

   All components of this strategy should be coordinated with our international partners – particularly the G-7 nations – to strengthen our ability to retaliate while raising the costs of hostile cyber actions against us.

**Post-Hearing Questions for the Record**
**Submitted to Eric Rosenbach**
**From Senator Heidi Heitkamp**

**"Mitigating America's Cybersecurity Risk"**

**April 24, 2018**

1. Mr. Rosenbach, you have taken steps to evaluate state cybersecurity efforts in response to lessons learned from and since the 2016 elections.

   a. **Do you believe broadly that states have taken the necessary steps to prevent and respond to cyberattacks during the course of the 2018 election? If not, do you believe that most states will have taken these steps prior to election day in November?**

   The states have made important progress since 2016 and have demonstrated continued improvements, but they remain challenged by inadequate resources, the diversity of the election processes and infrastructure, and the complexity of establishing roles and responsibilities with the federal government. Most importantly, states require greater resources and federal support to successfully combat malicious cyber adversaries – a state-level election operation simply cannot be expected to defend itself against the Russian intelligence services. Additionally, the diversity of local election processes and operations make it challenging for an individual state to implement the same digital upgrades and patches across the board.

   b. **Broadly speaking, what are the largest gaps that still exist in state-level electoral cybersecurity? How do states collaborate better with the DHS and the federal government to close these gaps? In a best-case scenario, how long would it take to close the most glaring gaps prior to the elections in November?**

   Three complex problems remain pressing: many states need to improve standards for vendor selection and maintenance, should strengthen election auditing, and improve incident response strategy. These gaps are cause for substantial national security concern. As states work to close these gaps, leadership from the most senior election officials – secretaries of state, election board members, state election directors, and local election administrators – will be crucial in setting the tone for how the rest of the staff should prioritize system defense and protection.

   The biggest challenge to productive state-federal collaboration during this process is balancing the need for states to take action to address the threat against the need for some measure of federal support. After initial friction with the states, the designation of election systems as critical infrastructure has helped smooth the path for money and resources to flow from DHS to the states, but state and federal governments must delineate their crisis management roles and responsibilities when it comes to elections and establish how those resources will be spent on security upgrades. DHS has made solid progress in building trust with the states over the past year, and the rest of the federal government must not damage that trust. However, states can and should draw on the assets of the National Guard and their DHS fusion centers to improve information sharing and intelligence regarding threats and the capabilities available to them to counter these threats.

In the event of future attacks on our election systems, both federal and state officials must get their facts right when going to the public if we are to maintain their trust. Too much of the aftermath of the 2016 election interference was characterized by delayed disclosures; the 21 states that were targeted still have not been publicly identified, which has fueled accusations and mistrust among suspicious members of the public. The states must engage skilled public relations professionals trained in crisis communications who can build key links to the public during this kind of crisis.

2. I am also deeply concerned about cyberattacks on our nation's electrical grid and facilities – and more broadly our energy infrastructure, including pipelines, drilling rigs, and numerous other components and tools of our vast energy industry. Russia has already attacked the energy systems in Ukraine – and we know that several state actors have been discovered rooting around in the systems of various U.S. utilities, facilities, and energy infrastructure.

    a. **Where would you say these systems and facilities rank in terms of priorities for foreign state actors? Are the companies and owners of these targeted facilities treating the threat appropriately to match this prioritization by foreign state actors?**

    The interconnectedness of our energy systems renders them a high priority target for the advanced offensive cyber capabilities of foreign adversaries like Russia, North Korea and Iran. The attacks in Ukraine were clear proof of Russia's interest in targeting critical infrastructure sectors, and the methods used by hackers to do so grow only more sophisticated. So far, private sector cybersecurity firms has been more agile in its response to the latent threat than the federal government. The United States deterrence posture on this issue is nearly non-existent. . The number of vulnerabilities and the interest of our adversaries demand that the companies and owners of high-risk targets begin to take the threat even more seriously.

    b. **What are your biggest concerns related to cyberattacks on these systems and infrastructure? Are we doing enough at the federal and state government level to address these challenges?**

Potential attacks on our energy systems constitutes a "whole of nation" threat that requires a "whole of nation" response. No single organization can defeat this challenge alone, and federal and state government responses must be coordinated with private sector and non-governmental actors to achieve success.

The cyber workforce and its leadership will be key to addressing these challenges, and currently there is substantial room for improvement. The White House recently eliminated the position of cybersecurity coordinator, creating a leadership void that makes it more difficult to execute the mission of combating cyber threats and investing in lessons learned and resiliency. We need to maintain a long-term pipeline of cyber-security talent in the government equipped to address these challenges.

c. **What more can the federal government do to assist utilities, facility owners, and energy infrastructure in preparing for, responding to, and sharing information about cyberattacks?**

As part of a "whole of nation" approach, the federal government should increase information sharing with high-risk targets and industries to improve preparation and ability to respond. It should support these companies with capabilities, including cybersecurity scans and risk assessments. To encourage collaboration from the private sector, the federal government will need to balance regulatory action with market incentives. On the regulatory front, Congress should mandate that all critical infrastructure providers adopt the NIST Cybersecurity Framework and standardize security protocols for the manufacturers and distributors of office devices used in the industry. By improving collection and access to cyber incident data, government actors can lay the foundation for a cyber insurance market, which will be a key tool in improving risk management by critical infrastructure providers.

3. During the hearing, I appreciated your comments regarding congressional oversight of DHS. Senator Johnson and I have expressed our concerns about the complexity of the current oversight structure and how it can lend itself to gridlock, gaps in oversight, and inefficient oversight. Streamlining congressional oversight of DHS is a legitimate national security challenge, and we need to address it.

a. **In your view, what steps should Congress take to streamline congressional oversight of DHS?**

While a transparent and responsive working relationship between Congress and DHS serves the interests of the American people, the current convoluted oversight structure detracts from DHS's ability to carry out its mission. Consolidating the number of committees overseeing DHS would be a logical first step to improving oversight efficiency and effectiveness. Over 100 committees and subcommittees claim jurisdiction over DHS – nearly three times more than over DoD, a much larger organization with a much more substantial budget – and each claim carries unique reporting requirements. Answering each annual requirement and testifying at hearings diverts resources and labor hours away from the Department's critical operational efforts to protect the homeland. The country stands to benefit from clarifying and repairing this fractured oversight structure so that DHS is empowered to devote its resources to operational work. Passing the DHS Authorization Act (H.R.2825), currently awaiting action in the Senate, would be a first logical step to reduce the stranglehold of oversight mechanisms.

Congress can amplify improvements from this streamlining by committing to the provision of adequate funding and necessary authorities. Ensuring proper resourcing and an optimized internal structure – such as through the creation of an operationally-focused cybersecurity agency to support critical infrastructure operators, or by permitting component name changes to proceed without an act of Congress – would create efficiency in DHS's internal structure and simplify oversight. Taken jointly, these organizational reforms will improve DHS's ability to mitigate the risks of cyberattacks by our adversaries.